2010 - 2011 - 2012

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

PRIVACY AMENDMENT (ENHANCING PRIVACY PROTECTION) BILL 2012

EXPLANATORY MEMORANDUM

(Circulated by authority of the Attorney-General,
the Honourable Nicola Roxon, MP)

PRIVACY AMENDMENT (ENHANCING PRIVACY PROTECTION) BILL 2012

OUTLINE

This Bill amends the *Privacy Act 1988* to implement the Government's first stage response to the Australian Law Reform Commission's (ALRC) report number 108, called 'For Your Information: Australian Privacy Law and Practice' (ALRC Report). Given the large number of recommendations, the Government announced that it would respond to the ALRC report in two stages. The Government's first stage response addressed 197 of the ALRC's 295 recommendations. The Bill implements the major legislative elements of the Government's first stage response.

The Bill amends the Privacy Act to:

- Create the Australian Privacy Principles (APPs), a single set of privacy principles applying to both Commonwealth agencies and private sector organisations (referred to as APP entities), which replace the Information Privacy Principles (IPPs) for the public sector and the National Privacy Principles (NPPs) for the private sector
- Introduce more comprehensive credit reporting with improved privacy protections, at the same time rewriting the credit reporting provisions to achieve greater logical consistency, simplicity and clarity and updating the provisions to more effectively address the significant developments in the operation of the credit reporting system since the provisions were first enacted in 1990
- Introduce new provisions on privacy codes and the credit reporting code (called the CR code), including powers for the Commissioner to develop and register codes in the public interest that are binding on specified agencies and organisations; and
- Clarify the functions and powers of the Commissioner and improve the Commissioner's ability to resolve complaints, recognise and encourage the use of external dispute resolution services, conduct investigations and promote compliance with privacy obligations.

The Bill introduces modifications to the Act as recommended by the ALRC. The APPs set out standards, rights and obligations in relation to the handling and maintenance of personal information by APP entities, including dealing with privacy policies and the collection, storage, use, disclosure, quality and security of personal information, and access and correction rights of individuals in relation to their personal information. As recommended by the ALRC, the APPs and credit reporting provisions are structured to more accurately reflect the 'life cycle' of personal information.

The Bill introduces a number of additional safeguards for the protection of privacy, including enhanced notification, quality, correction, and dispute resolution mechanisms for individuals.

Structure of the Bill

The substantive elements of the reforms are contained in six schedules to the Bill. Each schedule deals with a particular subject and related matters, including related definitions. The schedules and their topics are:

- Schedule 1 – Australian Privacy Principles
- Schedule 2 – Credit reporting
- Schedule 3 – Privacy codes
- Schedule 4 – Other amendments of the *Privacy Act 1988*

- Schedule 5 – Amendment of other Acts
- Schedule 6 – Application, transitional and savings provisions

Schedule 1 – the Australian Privacy Principles

Schedule 1 of the Bill amends the Privacy Act to create the APPs, a single set of privacy principles applying to APP entities, a term that refers to both Commonwealth agencies and private sector organisations. To facilitate ease of reference to the APPs and minimise confusion around numbering that may result if they were sections of the Act, they are inserted as a schedule to the Act.

The APPs are grouped into five sets of principles:

1. Principles that require APP entities to consider the privacy of personal information, including ensuring that APP entities manage personal information in an open and transparent way (APP 1, APP 2)
2. Principles that deal with the collection of personal information, including unsolicited personal information (APP 3, APP 4, APP 5)
3. Principles about how APP entities deal with personal information and government related identifiers, including principles about the use and disclosure (including cross-border disclosure) of personal information and identifiers (APP 6, APP 7, APP 8, APP 9)
4. Principles about the integrity, quality and security of personal information (APP 10, APP 11)
5. Principles that deal with requests for access to, and correction of, personal information (APP 12, APP 13).

Schedule 1 also deals with a range of amendments relating to the APPs, including amendments to update or insert new definitions. One key term that has been updated is 'personal information'.

Schedule 1 also repeals Divisions 2 and 3 of Part III of the Act. These divisions provide for the application of the IPPs, the NPPs and approved privacy codes. The IPPs and NPPs will be replaced by the APPs. A new Part IIIB will be inserted into the Act dealing with privacy codes.

Schedule 2 – Credit Reporting

The *Privacy Amendment Act 1990*, which commenced in September 1991, extended the coverage of the Privacy Act to consumer credit reporting. The credit reporting provisions of the Privacy Act are contained in Part IIIA and associated provisions (the credit reporting provisions). The credit reporting provisions primarily regulate the handling and maintenance of certain kinds of personal information concerning consumer credit that is intended to be used wholly or primarily for domestic, family or household purposes.

The purpose of the credit reporting system is to balance an individual's interests in protecting their personal information with the need to ensure sufficient personal information is available to assist a credit provider to determine an individual's eligibility for credit following an application for credit by an individual, and for related matters. The credit reporting system provides an aid to credit providers in managing the risks of providing consumer credit to individuals. Only limited and defined kinds of relevant personal information are permitted in the credit reporting system.

The credit reporting system in Australia has been a 'negative' reporting system. The main kinds of personal information permitted in the system were information about:

- a credit provider having sought a credit report regarding an individual in connection with an application for credit, and the amount of credit sought in the application
- an individual's current credit providers
- any credit defaults; and
- a credit provider's opinion that the individual has committed a serious credit infringement.

Schedule 2 amends the credit reporting provisions in the Privacy Act. The credit reporting provisions have been completely revised, consistent with the intention to ensure greater logical consistency, simplicity and clarity throughout the Privacy Act. The new provisions are based on the flows of personal information in the credit reporting system and also clearly address the interaction of the provisions with the APPs where relevant.

This schedule of the Bill implements the ALRC's recommendation to move to a 'more comprehensive' credit reporting system. This means a limited number of additional kinds of credit related personal information about individuals are permitted in the credit reporting system. The five new kinds of personal information (also known in the industry as 'data sets') are:

- the date the credit account was opened
- the type of credit account opened
- the date the credit account was closed
- the current limit of each open credit account; and
- repayment performance history about the individual.

The fifth kind of personal information, repayment history information, is only available to credit providers who are licensees under Chapter 3 of the National Consumer Credit Protection Act and subject to responsible lending obligations under that Chapter. In certain defined circumstances repayment history information is also available to mortgage insurers for mortgage insurance purposes.

Comprehensive credit reporting will give credit providers access to additional personal information to assist them in establishing an individual's credit worthiness. The additional personal information will allow credit providers to make a more robust assessment of credit risk and assist credit providers to meet their responsible lending obligations. It is expected that this will lead to decreased levels of over-indebtedness and lower credit default rates. More comprehensive credit reporting is also expected to improve competition and efficiency in the credit market, which may result in reductions to the cost of credit for individuals.

The new credit reporting provisions will provide additional consumer protections by enhancing obligations and processes dealing with notification, data quality, access and correction, and complaints. This includes measures to place greater responsibility on credit reporting bodies and credit providers to assist individuals to access, correct and resolve complaints about their personal information. Other measures that will benefit individuals include the introduction of specific rules to deal with pre-screening of credit offers and the freezing of access to an individual's personal information in cases of suspected identity theft or fraud.

Schedule 3 – Codes

Schedule 3 replaces the provisions dealing with privacy codes and the Credit Reporting Code of Conduct with a new Part IIIB dealing with codes of practice under the APPs (called APP codes) and a code of practice about credit reporting (called the CR Code).

An APP code may be developed by APP code developers (either at their own initiative or following a request from the Commissioner) or by the Commissioner. APP codes do not replace the APPs, but operate in addition to the requirements of the APPs. An APP code must set out how one or more of the APPs are to be applied or complied with. An APP code may also deal with other relevant matters, and may impose additional requirements to those imposed by the APPs so long as the additional requirements are not contrary to, or inconsistent with, the APPs. Once the APP code has been developed an application may be made to the Commissioner for registration of the code. The Commissioner then decides whether or not to register the APP code. The Commissioner also has the power to develop an APP code. This power can only be exercised if the Commissioner has requested the development of an APP code and the request has not been complied with or the Commissioner has decided not to register the APP code that was developed as requested. The Commissioner may then register the APP code that was developed by the Commissioner.

Any APP code that is registered will be a disallowable legislative instrument. An APP entity that is bound by a registered APP code must not do an act, or engage in a practice, that breaches the registered APP code. A breach of the registered APP code will be an interference with privacy by the entity under section 13 of the Act and subject to investigation by the Commissioner under Part 5 of the Act. Registered APP codes can be varied or removed from the register.

The CR code is an essential part of the regulatory structure of the credit reporting system. Accordingly, the Commissioner will request code developers to develop the CR code. The development process is based on that used for APP. The CR code must set out how one or more of the credit reporting provisions are to be applied or complied with, and deal with other matters. The CR code must bind all credit reporting bodies and must set out which credit providers or other entities (for example, mortgage insurers and trade insurers) are bound. The Commissioner can develop the CR code if the code developers do not develop the CR code as requested, or the Commissioner decides not to register the CR code that was submitted for registration.

A breach of the registered CR Code will be an interference with privacy by the entity under section 13 and subject to investigation by the Commissioner under Part 5 of the Act. The registered CR code can be varied.

The Commissioner has certain functions and powers in relation to codes. The Commissioner must maintain the Codes Register, which contains the registered APP codes and registered CR code. The Commissioner may issue guidelines to provide assistance in the development of, and compliance with, APP codes and the CR code. The Commissioner may also make guidelines about matters the Commissioner may consider in deciding whether to register or vary an APP code or the CR code, or remove an APP code from the Register. The Commissioner may also review the operation of any registered codes.

Schedule 4 – Other amendments of the Privacy Act 1988

Schedule 4 inserts an objects clause into the Act, reforms the functions and powers of the Information Commissioner, and deals with related matters, including reform of the provisions on interferences with privacy. The amendments improve the Commissioner's ability to resolve complaints, recognise and encourage the use of external dispute resolution services,

conduct investigations and promote compliance with privacy obligations. The amendments also restructure relevant provisions dealing with the powers and functions of the Commissioner to improve clarity and consistency in the provisions.

A new provision sets out the general functions of the Commissioner. This is followed by provisions which outline in greater detail the guidance related functions of the Commissioner, the monitoring related functions of the Commissioner, and the advice related functions of the Commissioner. Relevant definitions related to the functions and powers of the Commissioner are also amended.

Other amendments to the Commissioner's powers and functions made by Schedule 4 include:

- Clause 33C will enable the Commissioner to conduct an assessment of an APP entity's maintenance of personal information
- Clause 33E will allow the Commissioner to accept written undertakings by entities to take, or refrain from taking, specified actions to ensure compliance with the Act
- Clause 35A will give the Commissioner the power to recognise external dispute resolution schemes
- Clause 40A will deal with the conciliation of complaints by the Commissioner
- Item 90 will extend the Commissioner's power to make inquiries of persons other than the respondent to a complaint; and
- Clause 52(3A) will allow the Commissioner to include in a determination any order that considered necessary or appropriate.

Schedule 4 also amends the provisions dealing with the extra-territorial operation of the Act. Subsection 5B(1) is amended to extend the extra-territorial operation of the Act and registered APP and CR codes to organisations and small businesses with an Australian link. The term 'Australian link' is used to define the entities that are subject to the operation of the Act, and is used, for example, in APP 8 and throughout the credit reporting provisions.

A new section 13G is inserted, to provide a civil penalty for a serious or repeated interference with the privacy of an individual. Schedule 4 also inserts a new Part VIB, which deals with civil penalties.

Schedule 5 – Amendment of other Acts

Schedule 5 contains amendments to other Acts that are consequential to the amendments in Schedules 1 to 4 of the Bill. These amendments primarily replace references to the IPPs or NPPS with the APPs and insert new definitions, including certain credit reporting terms, in other Acts that interact with the Privacy Act.

Schedule 6 – Application, transitional and savings provisions

Schedule 6 contains amendments to address transitional issues relating to the commencement of the new provisions.

Financial Impact Statement

The Bill will have no significant impact on Commonwealth expenditure or revenue.

Regulation Impact Statement

A regulation impact statement is only required for the credit reporting measures contained in this Bill.

REGULATION IMPACT STATEMENT – CREDIT REPORTING REFORMS

Background, purpose and structure of the Regulation Impact Statement (RIS)

Background

In 2006 the then Australian Government asked the Australian Law Reform Commission (ALRC) to conduct an inquiry into the extent to which the *Privacy Act 1988* (the Privacy Act) and related laws continue to provide an effective framework for the protection of privacy in Australia.

In August 2008 the ALRC report *For Your Information: Australian Privacy Law and Practice* (108) (the ALRC Report) was publicly released. The ALRC Report contains 295 recommendations for reform of the Privacy Act and related legislation, including recommendations relating to reform of the consumer credit reporting provisions (Part IIIA of the Privacy Act).

Over a two year period, the ALRC released an Issues Paper and Discussion Paper to assist in informing its recommendations in the final report. In developing the consumer credit reporting recommendations, the ALRC formed a Credit Reporting Advisory Sub Committee made up of Treasury officials, consumer advocates, credit provider representatives and credit reporting agency representatives. The ALRC consulted widely with community groups and the business community, seeking written submissions and conducting a series of roundtables with individuals, agencies and organisations about consumer credit reporting.

The ALRC recommendations on credit reporting contain two significant proposals:

1. **The current consumer credit reporting regime move to a system that includes 'more comprehensive' consumer credit information, as follows:**
    a. **Recommendation 55–1** The new *Privacy (Credit Reporting Information) Regulations* should permit credit reporting information to include the following categories of personal information, in addition to those currently permitted in credit information files under the *Privacy Act*:
        i. the type of each credit account opened (for example, mortgage, personal loan, credit card);
        ii. the date on which each credit account was opened;
        iii. the current limit of each open credit account; and
        iv. the date on which each credit account was closed.
    b. **Recommendation 55–2** Subject to Recommendation 55–3, the new *Privacy (Credit Reporting Information) Regulations* should also permit credit reporting information to include an individual's repayment performance history, comprised of information indicating:
        i. whether, over the prior two years, the individual was meeting his or her repayment obligations as at each point of the relevant repayment cycle for a credit account; and, if not,
        ii. the number of repayment cycles the individual was in arrears.
    c. **Recommendation 55–3** The Australian Government should implement Recommendation 55–2 only after it is satisfied that there is an adequate framework imposing responsible lending obligations in Commonwealth, state and territory legislation.

d. **Recommendation 55–4** The credit reporting code should set out procedures for reporting repayment performance history, within the parameters prescribed by the new *Privacy (Credit Reporting Information) Regulations*.

e. **Recommendation 55–5** The new *Privacy (Credit Reporting Information) Regulations* should provide for the deletion of the information referred to in Recommendation 55–1 two years after the date on which a credit account is closed.

2. A new credit reporting Code of Conduct be developed by industry, as follows:

a. **Recommendation 54–9** Credit reporting agencies and credit providers, in consultation with consumer groups and regulators, including the Office of the Privacy Commissioner, should develop a credit reporting code providing detailed guidance within the framework provided by the *Privacy Act* and the new *Privacy (Credit Reporting Information) Regulations.* The credit reporting code should deal with a range of operational matters relevant to compliance.

Purpose

The purpose of this RIS is to determine whether the proposed policy objectives in Recommendations 55-1 to 55-5 and 54-9 should be accepted and if so, the form in which the recommendations should be accepted.

Structure

The RIS begins by providing background on the issue of consumer credit reporting and summarises previous reviews. It then provides background on the issue of a credit reporting Code of Conduct. The RIS is then broken into two parts. Part A considers comprehensive credit reform, while Part B considers a credit reporting code of conduct. The RIS examines the problems, options and impacts to determine the most effective and efficient regulatory approach in relation to both of these issues.

Background to Consumer Credit Reporting

The credit reporting system is intended to increase the efficiency of Australia's consumer credit market. As of June 2008, total consumer credit on issue, including securitisations, was $1113.4 billion. Of this, housing credit on issue stood at $957.9 billion and other personal credit on issue was $155.6 billion. The largest sector of consumer credit is residential mortgages, which are estimated to account for over 86 per cent of all consumer loans.[1]

Within the consumer credit market credit providers obtain credit reports from credit reporting agencies (CRAs) to assist in the assessment of credit applications with the aim of minimising the risk of customer defaults.

CRAs collect information about individuals from credit providers and from publicly available sources (such as bankruptcy information obtained from the Insolvency and Trustee Service Australia). This information is used in generating credit reporting information for credit providers. Credit providers use this information when assessing credit applications, as it augments information obtained directly from an individual's application form, the credit provider's own records of past transactions involving the individual (if any), and any other enquiries the credit provider may choose to make.

Consumer credit reporting is regulated by Part IIIA of the Privacy Act. It regulates the types of personal information that may be collected and disclosed in the course of consumer credit reporting by a defined class of CRAs and credit providers. The Privacy Act allows for the collection and disclosure of 'negative' credit reporting information. Subsection 18E(1) of the Privacy Act sets out a prescriptive list of information which may be included in a credit information file. This includes:

- a credit provider having sought a credit report in connection with an application for credit, and the amount of credit sought (inquiry information)
- a credit provider being a current credit provider in relation to the individual (current credit provider status)
- credit provided by a credit provider to an individual, where the individual is at least 60 days overdue in making a payment on that credit (default information)
- a cheque for $100 or more that has been dishonoured twice
- a court judgment or bankruptcy order made against the individual; and
- a credit provider's opinion that the individual has committed a serious credit infringement.

In Australia there are currently three CRAs active:

- Veda Advantage (Veda)
- Dun and Bradstreet (D&B); and
- Tasmanian Collection Service

Veda claims a market share of 96%[2] with a database of 16.5 million credit-active Australians[3]. It is understood that Veda has over 5000 subscribers which use its services,

[1] National Consumer Credit Protection Bill 2009 Executive Memorandum p.363 at 10.3

[2] 'Veda Advantage responds to ALRC Privacy Review proposal' in *Wot News*, accessed 9 July 2009, from <http://wotnews.com.au/like/veda_advantage_responds_to_alrc_privacy_review_proposal/1666111/>

although these are not exclusively credit providers.[4] The next largest CRA, D&B, claims to have data on 2.8 million individuals in Australia and New Zealand.[5]

The circumstances in which CRAs can disclose personal information contained in a credit information file are specified in section 18K of the Act. In general terms, CRAs can only disclose to credit providers (which is defined by section 6 of the Act to include mortgage insurers and trade insurers). Section 11B of the Act sets out a more detailed definition of credit providers, which includes:

- banks
- any entity which provides loans or credit cards for a substantial part of its business or allow individuals to have goods or services on credit (more than seven days)
- an entity that provides loans (including by issuing credit cards), provided the Privacy Commissioner has made a determination in respect of such a class of entity
- a government agency that provides loans and is determined by the Privacy Commissioner to be a credit provider for the purposes of the Act
- a person who carries on a business involved in securitisation or managing loans that are subject to securitisation; or
- an agent of a credit provider while the agent is carrying on a task necessary for the processing of a loan application, or managing a loan or account with the credit provider.

The definition does not include debt collectors, real estate agents, employers and general insurers. CRAs are not permitted to provide credit reports to any organisations which do not fall within the definition of a credit provider.

National Reform of Consumer Credit Law

Australian Governments are working towards the reform of consumer credit law in Australia. COAG, the Council of Australian Governments, agreed in March and July 2008 to transfer consumer credit regulation to the Commonwealth. Subsequently, COAG agreed on 3 October 2008 to a two-stage plan to overhaul consumer credit laws. The first stage of the plan includes the development of a national licensing scheme for the consumer credit industry, enacting the Uniform Consumer Credit Code as a Commonwealth law, and reforming key credit regulation laws.

On 27 April 2009 the then Minister for Superannuation and Corporate Law, Senator Sherry, released the draft National Consumer Credit Protection Bill 2009 (the NCCP Bill) for public comment. The NCCP Bill was introduced into the Australian Parliament on 25 June 2009.[6] Amongst other things, the NCCP Bill proposes new responsible lending obligations for all consumer credit in Australia. ALRC Recommendation 55-3 suggested the Government only

---

[3] 'Veda Advantage 'About Us', accessed 23 July 2009, from < http://www.vedaadvantage.com/about-veda/au_our-data.dot>

[4] ALRC report at paragraph 55.21

[5] Dun & Bradstreet 'Company profile', accessed 23 July 2009 from < http://dnb.com.au/Header/About_Us/Company_profile/index.aspx#DB_Australia_and_New_Zealand>

[6] Announced by the Minister at: http://ministers.treasury.gov.au/DisplayDocs.aspx?doc=pressreleases/2009/002.htm&pageID=003&min=ceba&Year=&DocType=0 viewed 18 September 2009.

permit repayment performance history in the credit reporting system if responsible lending obligations were introduced.

The NCCP Bill introduces a set of responsible lending conduct requirements, which set a standard of expected behaviour for credit providers when they enter into a credit contract, or when they suggest a credit contract to a consumer or provide assistance to a consumer to apply for a credit contract. Compliance with the responsible lending laws will require an assessment and verification of a consumer's credit needs and financial circumstances, including that the consumer has the capacity to repay the financial obligations.

Past Reviews of Credit Reporting

The question of whether more comprehensive credit reporting (also known as positive reporting) should be introduced into Australia has been actively considered since the enactment of the credit reporting system in 1988. Following is a summary of these proposals and reviews.

Credit Reference Association of Australia (CRAA) proposal

In 1988 the CRAA stated it would augment its collection of credit reporting information by including information about the current credit commitments of individuals. The proposal was named the Payment Performance System (PPS)[7]. Under the PPS credit providers would supply CRAA with tapes containing their customers' credit accounts which would be merged with existing data every 30 to 60 days. The data would be placed in credit reports containing a complete listing of all a consumer's credit accounts, balances owing, and payment performance on every account during the previous 24 payment periods. It was proposed that payments 120 days or more overdue would automatically generate a default report.

The CRAA's proposal was rejected by the then Government on the grounds that it was a form of 'positive reporting' which was too intrusive to the privacy of individuals.

Financial System Inquiry (Wallis Report) Proposal (1997)

The Wallis Report stated that it was not in a position to assess whether the benefits of positive credit reporting outweighed the costs, but considered the potential benefits warranted a complete review of the issue. The Wallis Report recommended that the Attorney-General establish a working party to review the existing credit provisions of the *Privacy Act*.[8] No information is available on whether the recommended review occurred.

Senate Legal and Constitutional References Committee

In 2005 the Senate Legal and Constitutional References Committee reported on aspects of credit reporting as part of its inquiry into the Privacy Act. The Committee's report, *The Real Big Brother: Inquiry into the Privacy Act 1988*, found that no reform of the credit reporting provisions of the Privacy Act was required. The Committee recommended against introducing positive credit reporting in Australia, stating that[9]:

the experience with the current range of credit information has shown that industry has not run the existing credit reporting system as well as would be expected and it is apparent injustice can prevail. As mentioned elsewhere in this report, positive reporting is also rejected on the basis that it would magnify the problems associated with the accuracy and

[7] ALRC report paragraph 52.34
[8] ALRC report paragraphs 55.20 – 21, quoting Financial System Inquiry Committee, *Financial System Inquiry Final Report* (1997).
[9] ALRC report paragraph 55.23, quoting Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005).

integrity of the current credit reporting system. The privacy and security risks associated with the existence of large private sector databases containing detailed information on millions of people are a major concern.

The Australian Government's response to the Senate Committee's recommendation concerning credit reporting and stated that review of the credit reporting provisions would be included in the reference to the ALRC to review privacy law in Australia.

Senate Economics Committee

The Senate Economics Committee also considered the issue in its 2005 report *Consenting Adults, Deficits and Household Debt: Links between Australia's Current Account Deficit, the Demand for Imported Goods and Household Debt*. The Committee stated that it was not persuaded to take a different view to that expressed by the Senate Legal and Constitutional References Committee on the basis that[10]:

- credit providers were not making full use of the information available to them; and
- defaults in the credit card market and other signs of financial distress were very low and did not justify a move to positive credit reporting.

Victorian Consumer Credit Review

The 2006 Consumer Credit Review examined comprehensive credit reporting as part of a broad review of the efficiency and fairness of the operation of credit markets and the regulation of credit in Victoria. The Consumer Credit Review rejected a form of more comprehensive credit reporting on the basis that there were unanswered questions as to whether the benefits outweighed the costs. However it recommended that further research and analysis be undertaken on the effects of comprehensive credit reporting.

House of Representatives Standing Committee on Economics

In November 2008, after the publication of the ALRC Report, the House of Representatives Standing Committee on Economics' Inquiry Into Competition in the Banking and Non-Banking Sectors recommended that the Government implement the ALRC's recommendations on reforming Australia's credit reporting system. In particular, the report considered the effect of comprehensive credit reporting and concluded that adopting a comprehensive credit system would provide competitive advantages to both businesses and individuals. The report referred to The Treasury's findings which noted that the current negative credit reporting model may represent a barrier to competition as it prevents new entrants and smaller existing lenders from obtaining comprehensive information on a prospective customer's ability to service a loan and that only a 'customer's existing lender…has access to the borrower's repayment history'.[11]

Background to Credit Reporting Code of Conduct

Section 18A of the Privacy Act requires the Privacy Commissioner to issue a Code of Conduct relating to credit information files and credit reports. The Privacy Commissioner is

[10] ALRC report paragraph 55.25

[11] House Standing Committee on Economics: Inquiry into competition in the banking and non-banking sectors http://www.aph.gov.au/house/committee/economics/banking08/report/Fullreport.pdf at 3.138 accessed 16/07/09

required to consult with government, commercial, consumer and other relevant bodies and organisations before issuing the Code of Conduct. The Code of Conduct should deal with:

- the collection of personal information for inclusion in individuals' credit information files
- the storage of, security of, access to, correction of, use of and disclosure of personal information included in individuals' credit information files or in credit reports
- the manner in which credit reporting agencies and credit providers are to handle disputes relating to credit reporting; and
- any other activities, engaged in by CRAs or credit providers, that are connected with credit reporting.

The Privacy Commissioner issued the *Credit Reporting Code of Conduct* in 1991. The Code supplements Part IIIA on matters of detail not addressed by the Privacy Act. Among other matters, the Code requires credit providers and CRAs to:

- deal promptly with individual requests for access and amendment of personal credit information, such as proscribing specific timeframes within which requests must be dealt with
- ensure that only permitted and accurate information is included in an individual's credit information file
- keep adequate records in regard to any disclosure of personal credit information
- adopt specific procedures in settling credit reporting disputes, and
- provide staff training on the requirements of the Privacy Act.

The Code supplements Part IIIA of the Privacy Act and creates a set of legally binding rules. Subsection 18A(4) states that the Code of Conduct is a disallowable instrument. Section 18B of the Act requires CRAs and credit providers to comply with the Code of Conduct.

The term 'credit providers' is defined in section 11B of the Privacy Act. The definition extends to an organisation that is, among other things, a:

- bank
- corporation, a substantial part of whose business or undertaking is the provision of loans
- corporation that carries on a retail business in the course of which it issues credit cards; or
- corporation that provides loans and is included in the class of corporations determined by the Privacy Commissioner to be credit providers for the purposes of the Privacy Act.

The term 'loan' is defined in section 6(1) of the Privacy Act to mean a contract, arrangement or understanding under which a person is permitted to defer payment of a debt, and includes a hire-purchase agreement or an agreement for the hire, lease or renting of goods or services.

The Privacy Commissioner has issued two determinations in relation to the definition of credit provider. These are the *Credit Provider Determination No. 2006-4 (Classes of Credit Providers)* and the *Credit Provider Determination No. 2006-3 (Assignees)*. These

determinations state circumstances in which corporations are to be regarded as credit providers. They include situations where corporations make loans in respect of the provision of goods or services on terms that allow the deferral of payment, in full or in part, for at least seven days.

The operation of the Privacy Act and the Privacy Commissioner's Determinations means that the type of corporations that may be included within the definition of credit provider has been considerable expanded. Submissions to the ALRC recognised that organisations which are retailers or service providers, such as video store operators or legal and healthcare service providers, may fall within the definition of credit provider if they extend payment terms for seven days or more[12]. In some situations, organisations that would otherwise be small businesses may be caught by the operation of the credit reporting provisions.

[12] ALRC Report paragraph 54.112

PART A: Comprehensive Credit Reporting

1. Problem

1.1 Greater access to independent credit information

A key objective of credit reporting is to facilitate consumer credit transactions by encouraging transparency in the market and providing access to standardised, reliable and timely information about an individual's credit risk.[13] A significant concern in the consumer credit industry is that the existing credit reporting system does not sufficiently address the information asymmetry between credit providers and potential borrowers. Information asymmetry occurs where the credit provider does not know the full credit history of an individual applying for credit and therefore the individual has more information about his or her credit risk than the credit provider. This can result in adverse selection, where a credit provider operating in response to information asymmetry, prices credit based on the *average* credit risk of individuals.[14] The credit reporting system attempts to address this information asymmetry by providing an independent source of information that can assist in the assessment of an individual's credit application.

The present credit reporting system in Australia is a negative credit reporting type of system, as opposed to the 'positive' credit reporting type of system permitted in other countries. The difference between the two systems is the type of personal information which is permitted to be collected. Negative reporting limits the collection of personal information to that which relates to an individual's credit delinquency, such as defaults on payments or dishonoured cheques, and inquiries on the credit record. Positive credit reporting permits the collection of personal information which demonstrates an individual's credit account activity, such as the timeliness of payments, account type, the credit limit and the amounts of credit liabilities. However, the terms positive reporting and negative reporting are not clearly defined and can be confusing. The ALRC uses the term 'comprehensive credit reporting' to describe the inclusion of additional information which would feature in a positive credit reporting system.

It is argued by the credit reporting industry that Australia's current credit reporting system provides insufficient credit history information about an individual. They argue this may cause credit providers to incorrectly assess the risk premium of individuals when they apply for credit, which can cause the following consequences:

- granting credit, or higher amounts of credit, to individuals who cannot afford to meet their repayment obligations
- not granting credit, or less credit than desired, to individuals who can afford to meet their repayment obligations

Industry stakeholders argue that the lack of more comprehensive information may mean they are ignorant of the fact that an individual's circumstances may have changed and therefore their ability to repay has changed. Credit providers are forced to place a lot of emphasis on current information contained in credit reports, such as default listings, which do not accurately reflect an individual's credit risk. A minor default is recorded for a period of 5 years after the event, but information about an individual's changed circumstances, such as evidence of consistent and timely repayment of debts, is not recorded. Overall, it is argued there is an information asymmetry which results in the mis-pricing and mis-allocation of credit.[15] In consultations industry stakeholders have suggested that the absence of more

[13] M Miller, *Credit Reporting Systems and the International Economy*, 2003, p 410.
[14] ALRC Report paragraph 52.17
[15] Dun & Bradstreet, Submission to Senate Economics Reference Committee Inquiry into Possible

comprehensive credit reporting may affect the price of credit (both in the consumer credit market as a whole and for individual consumers) which affects the availability of credit. They also argue that the lack of more comprehensive credit information may lead to more defaults, as customers who would not have qualified for credit may be able to obtain credit in the current negative credit reporting system by exploiting the information asymmetry which makes it difficult for credit providers to discover information about an applicant's true financial position.

There does not appear to be independent empirical information available about the Australian consumer credit reporting system, industry, or the implications of more comprehensive credit reporting. The lack of independent information was noted by the ALRC.[16] Independent information was not available in the preparation of this RIS.

While the major purpose of credit reporting is to provide information to assist credit providers to assess applications for credit, an effective credit reporting system may also facilitate responsible lending by credit providers, helping to ensure individuals do not become financially overcommitted. The National Consumer Credit Protection Bill 2009 [which has since passed as the *National Consumer Credit Protection Act 2009*] proposes extensive responsible lending obligations which will require credit providers to ensure they adequately and responsibly assess an individual's application for credit.

1.2 Privacy concerns

Permitting access to more credit information through the credit reporting system directly affects an individual's privacy. The main concerns from consumer and privacy advocate stakeholders and some commercial stakeholders are:

- the benefit of comprehensive credit reporting does not outweigh the additional impact on an individual's privacy
- CRAs will have access to large databases of personal information
- comprehensive credit information may be used for purposes unrelated to assessing the creditworthiness of an applicant for credit, such as marketing or other unauthorised purposes, including identity fraud
- there may be an increased risk that information will be inaccurate due to the greater volume of information (reflecting existing concerns about accuracy of the currently held credit reporting information) and any inaccuracies may make it more difficult for individuals to obtain credit
- based upon evidence from overseas, there is an increased risk that the security of data held by CRA's will be compromised; and
- it would be inappropriate for CRA's to collect and report payment performance information in relation to utilities such as telecommunications, energy and water.

2. Objectives

2.1 *Objectives of government action*

The objective of government action is to respond to the ALRC recommendations on consumer credit reporting reform in the context of the Government's response to the wider ALRC review of privacy law. The specific objectives are to:

Links between Household Debt, Demand for Imported Goods and Australia's Current Account Deficit, March2005

[16] ALRC report paragraph 55-108

- provide consumer credit providers with sufficient information to allow them to adequately assess credit risk while ensuring the protection of personal information to the greatest extent possible; and
- encourage responsible lending.

2.2 *Existing policy and regulations*

Part IIIA of the Privacy Act precisely defines the categories of personal information which may be collected and disclosed for credit reporting purposes. The policy objective of the existing credit reporting system is to provide a mechanism to allow a limited amount of personal information to be collected and disclosed in the credit reporting system for the efficient operation of the consumer credit market.

The ALRC has recommended changes to the existing credit reporting system in order to permit more comprehensive credit reporting. Amendments would be required to Part IIIA of the Privacy Act.

3 Options that may achieve the objectives

3.1 *Implementation scope*

Part IIIA of the Privacy Act regulates the consumer credit reporting system. Against this background, the proposed options address the ALRC's recommendations 55-1 and 55-2 on adopting a more comprehensive consumer credit reporting system within the Privacy Act. The scope of implementation is limited to amending, or not amending, Part IIIA of the Privacy Act.

The ALRC considered options to make the current credit reporting system more effective[17]. These options included improving the accuracy of existing credit reporting data, requiring consumer declarations in relation to loan applications and expanding financial literacy programs. However, the ALRC did not recommend any of these options for action and accordingly this RIS does not consider these options.

Implementation of the ALRC recommendations would enable CRAs to collect additional information. However, CRAs would not be obliged to collect additional information. It is expected that CRAs will only incur any costs in collecting additional information (whether through redeveloping systems or for other reasons) if they expect the benefits of collecting more comprehensive credit information to outweigh the costs.

3.2 *Option 1 – Maintain the current permitted categories of credit reporting information, retaining a negative credit reporting system (the status quo)*

This option retains the current permitted categories of negative credit reporting information. No amendments would be made to Part IIIA of the Privacy Act.

3.3 *Option 2(a) – Move towards a more comprehensive credit reporting system by including four additional categories of personal information*

This option would permit credit reporting information to include the following categories of information, in addition to those currently permitted under Part IIIA of the Privacy Act:

- the type of each credit account opened (for example, mortgage, personal loan, credit card)
- the date on which each credit account was opened

[17] ALRC Report paragraph 55.136

- the current limit of each open credit account, and
- The date on which each credit account was closed.

This option is based on Recommendation 55-1 from the ALRC Report.

3.4 *Option 2(b) - Expand the permitted outlined in Option 2(a) with the addition of including an individual's repayment history*

In addition to the four additional categories of personal information from Option 2(a), this option would also allow limited repayment history information to be included, as follows:

- whether, over the prior two years, the individual was meeting his or her repayment obligations as at each point of the relevant repayment cycle for a credit account; and, if not,
- the number of repayment cycles the individual was in arrears.

Note that the *amount* of any payments missed would not be included. This option is based upon Recommendation 55-2 of the ALRC Report, which recommends this option only be considered where there also exists an adequate legislative framework imposing responsible lending obligations on credit providers**.**

4. Assessment of impacts

4.1 *Impact group identification*

The groups affected by the Options are:

- individuals who apply for credit
- CRAs
- credit providers; and
- small businesses.

The Office of the Privacy Commissioner (the OPC) would remain the responsible regulator under all of the proposed options. It is expected that Options 2 and 3 would only have no, or a low, impact upon the OPC.

4.2 *Assessment of costs and benefits*

4.2.1 Impact of Option 1 – remain with status quo

Individuals - Benefits

The current protections in the Privacy Act limit the amount of personal data that may be collected, used and disclosed for the purpose of credit reporting. These limitations reduce the risk of data inaccuracy, misuse for marketing or other unauthorised purposes, or misuse for illegal activity, including identity fraud.

Individuals - Costs

The limited information available in credit reports may misrepresent the credit worthiness of individuals. For example, small defaults for small amounts of credit remain on a credit report for five years and may form the basis of a decision to approve credit, even where this default may be trivial in contrast to the overall credit history of an individual.

There is a risk that consumer credit may be priced at a higher rate than would otherwise be the case if more comprehensive credit information was available. There is also a risk that consumers may be denied credit or only have reduced credit made available because credit

providers may not have sufficient information to make fully effective decisions about the risks associated with the allocation of credit in the market as a whole or in relation to individual consumers.

Credit Reporting Agencies - Benefits

No requirements to change current data retention practices, business models or database technology.

Credit Reporting Agencies - Costs

Current regulation prevents CRAs from offering more comprehensive consumer credit reports which may limit the greater profitability of CRAs.

The current limited number of information categories may create competition costs by maintaining barriers to market entry for new CRA businesses. Two of the existing CRAs have large databases. Credit providers are more likely to use these CRAs as the size of the databases gives them access to the greatest potential number of consumer credit records. This may limit new entrants into the market because it is likely to take more time to develop databases of negative events like credit defaults.

Credit Providers - Benefits

No requirements to change current use and disclosure practices in relation to credit reporting information, business models or credit assessment technology.

Credit Providers - Costs

If an applicant fails to disclose credit accounts and liabilities they hold with other financial institutions, the credit provider is unable to make a fully informed lending decision resulting in the possibility of provision of credit to borrowers who are unable to meet their financial obligations.

New entrants into the credit provider market may face significant barriers to entry as a consequence of insufficient information about the credit risk of prospective credit consumers. New players or smaller credit providers are unlikely to have more comprehensive data available, while existing larger credit providers are able to access their existing customer base. This may mean knowledge of credit worthiness of individuals is inadequate which may lead to greater default rates for new and small credit providers**.**

Small Businesses - Benefits

To the extent that small businesses currently use the credit reporting system, they would not be required to make any changes.

Small Businesses - Costs

Small businesses may wish to use more comprehensive credit reporting information to provide greater certainty in the provision of credit to customers. Maintaining the current negative credit reporting system may place small businesses at proportionally greater risk from defaulting credit customers. No information is available on the extent of small business usage of the credit reporting system so it is not possible to quantify the possible costs.

4.2.2 Impact of Option 2(a) - Expand the permitted categories to include four additional categories of personal information

Individuals - Benefits

Permitting additional information provides the opportunity for credit providers to better understand an individual's credit history. In turn this may:

- result in lower rates of over-indebtedness and default
- allow individuals who are credit worthy to gain access to more appropriately priced credit (assuming credit providers introduce differential pricing)
- increase the availability of lending (to the extent that lenders currently limit the availability of credit due to the lack of more comprehensive credit reporting information)
- reduce the transaction costs in assessing credit applications, which could result in reduced costs to consumers if the cost savings are passed on by credit providers, and
- allow for greater automation and a faster credit decision making process, assuming credit providers change existing practices.

The extent to which price benefits (lower rates) would be realised by consumers depends in part on the level of competition in the consumer credit market - the greater the level of competition, the more likely that the benefits of comprehensive credit information would be passed on to consumers. While the magnitude of consumer benefits is uncertain, it is noted that currently there does not appear to be extensive competition in the consumer credit sector, raising some doubt that consumers would realise significant price benefits, at least over the short term.[18] Consumers may, however, benefit from greater access to credit.

Individuals - Costs

Individuals who are deemed to be a poor risk based on greater transparency about credit worthiness may find that the face a higher price for access to credit (assuming credit providers introduce differential pricing).

Permitting additional categories of personal information to be collected, used and disclosed may increase the risk of data inaccuracy, misuse for marketing or other unauthorised purposes, including identity fraud. If there are no significant changes to the numbers of CRAs operating in Australia, extremely large amounts of data about individuals will be held and maintained by a small number of CRAs which may increase the risk of data security challenges and the consequences of any potential breaches. Information is not available to quantify the possible cost of data inaccuracy. In many instances, the cost to any individual that may be affected by inaccurate records will not be obvious as individuals may resolve the issue by dealing directly with the credit provider or the CRA.

Credit Reporting Agencies - Benefits

The business model and marketability of CRAs is expected to be improved by allowing them to collect, use and disclose a greater amount of data on individuals who apply for credit, in turn giving CRAs the opportunity to sell a more effective product.

[18] Almost all new mortgages in July 2009 were written by the 'big four' banking groups, compared with around 60 per cent prior to the credit crisis (The Age 2009). As noted earlier, mortgages make up approximately 86 per cent of all consumer loans.

Credit Reporting Agencies - Costs

CRAs are likely to incur financial costs associated with developing systems to handle the additional information. However, CRAs can make commercial decisions about how they raise funds to invest in building systems to expand their systems and business operations and how they decide to recoup any investments they chose to make. CRAs may choose to off-set the investment costs against fees obtained from allowing credit providers to access the more comprehensive credit reporting information. For example, they may change their fee structure, market their services to a broader range of credit providers, or develop new services to market to their existing client base of credit providers. CRAs have not provided any information on the commercial decisions they may make to address any costs.

Credit Providers - Benefits

Access to more comprehensive credit reporting information is expected to allow credit providers to more accurately assess the risks involved in lending to an individual and in turn to more appropriately price credit. More information will allow credit providers to avoid lending to those who are over-committed, leading to lower rates of customer indebtedness and defaults and reducing costs for credit providers in debt recovery and write-offs.

Access to more comprehensive credit reporting information will provide a more efficient tool for credit providers to comply with responsible lending obligations under consideration in the NCCP Bill.

Access to more comprehensive credit reporting information may improve competition in the consumer credit provider market by reducing information asymmetry between credit providers, particularly between larger and smaller credit providers. Currently, large credit providers are able to access more comprehensive credit information from their own customers and use this to assess credit applications from their existing customers. In a more comprehensive credit reporting system, small credit providers may use the access to greater information to make more informed decisions about the provision of their credit which may make their businesses more competitive. It may also be the case that all credit providers may be able to reduce the transaction costs involved in assessing credit applications, creating a more efficient credit market.

Credit Providers - Costs

The systems and processes used by credit providers to assess credit applications may change to deal with access to more comprehensive information. If systems and processes change this may result in some costs for credit providers.

There may be higher costs to access credit information if CRAs choose to increase fees to off-set the costs of developing their systems. It is not possible to quantify these costs as this will be a commercial decision for CRAs and there is no information available on what choices CRAs may make to recoup any additional costs they may incur in updating their systems.

There may be a risk that the increased predictive value of the data available under this option may not be sufficient to justify the costs of implementation.

Small Businesses - Benefits

To the extent that small businesses currently use the credit reporting system, access to more comprehensive credit reporting information is expected to allow small businesses to more accurately assess the risks involved in lending to an individual. More information will allow

small businesses to avoid lending to those who are over-committed, leading to lower rates of customer indebtedness and defaults.

Small Businesses - Costs

Although there is no information available on the number of small businesses that currently use the credit reporting system, more small businesses may wish to use more comprehensive credit reporting information to provide greater certainty in the provision of credit to customers. Small businesses may face costs in developing processes to assess credit applications with access to more comprehensive information.

There may be higher costs to access credit information if CRAs choose to increase fees to off-set the costs of developing their systems. It is not possible to quantify these costs as this will be a commercial decision for CRAs and there is no information available on what choices CRAs may make to recoup any additional costs they may incur in updating their systems.

4.2.2.1 Research on credit market efficiency and macro-economic impact of more comprehensive credit reporting

In examining the introduction of comprehensive credit reporting the ALRC considered economic analysis provided by industry stakeholders. Broadly, stakeholders in support of comprehensive credit reporting claim that empirical and macro-economic studies provide important evidence about the likely improvements to credit market efficiency and economic benefits of comprehensive credit reporting.

The ALRC did not commission any independent economic analysis on the question of the possible macro-economic impact of credit reporting systems. The ALRC noted that, on one view:

this subject matter does not lend itself to precise modelling due to the level of complexity and the small orders of magnitude involved in terms of benefits. It is questionable whether any modelling will provide definitive answers.[19]

The Treasury has confirmed the ALRC views that data constraints restrict the level of macro-economic modelling that can be done on the possible impact of more comprehensive credit reporting. However, analysis conducted by Treasury has found that the introduction of positive credit reporting would be expected to remove information asymmetries in the market and lead to some small equity and efficiency benefits for credit market participants and the Australian economy more broadly.[20] The Treasury supports the introduction of comprehensive credit reporting subject to sufficient privacy protections being put in place.

4.2.2.2 Empirical studies on credit market efficiency with more comprehensive credit reporting

International comparative studies

Research by Barron and Staten published in 2000 compared Australia's credit reporting rules with that of the United States (US).[21] The research compared the accuracy of risk scoring models using the wider credit reporting information available under the US system with the more limited information available in Australia. The US model of credit reporting includes

[19] ALRC report paragraph 55.108
[20] The Department of Treasury *Submission to the ALRC Review of the Privacy Act 1988* December 2007
[21] J Barron and M Staten, *The Value of Comprehensive Credit Reports: Lessons from the US Experience* (2000) Online Privacy Alliance www.privacyalliance.org/resources/staten.pdf; referred to by submissions to the ALRC and viewed and cited by the ALRC report at paragraph 55.94 and 55.95.

information such as the type of account, credit limit, payment history, employer and account balance.

The findings of the research were that more comprehensive credit reporting rules resulted in fewer loan defaults while maintaining the same loan approval rate. The report found, for example, that at an approval rate of 60%, use of the credit reporting information permitted at present in Australia produced a default rate of 3.35% compared to a default rate of 1.9% in the US. At the same time, assuming that default rates were maintained at around the same rate (eg 4%), credit providers using information available in the current Australian system would extend new credit to 11,000 fewer consumers for every 100,000 applicants than would be the case in the US under their credit reporting system.

Later research by Barron and Staten, conducted in 2007 at the request of the Australian Finance Conference, compared the above findings with three other possible credit reporting models.[22] The research found that at the targeted approval rate of 60%, the intermediate model (similar to Option 2(b)) produced a 2.46% default rate. The ALRC notes the assertions that the implications of the research are that consumer credit will be less available and more expensive in countries, such as Australia, where the credit reporting system omits information that would provide a more complete picture of a consumer's financial position.[23]

The findings in the Barron and Staten research appear to be supported by other reports which broadly compared different credit systems in different countries. Research referring to overseas data demonstrated a lower default rate and reduced bankruptcies following the introduction of comprehensive credit reporting in several countries. For example, econometric research analysing the credit reporting regimes and credit markets in 43 countries, including the US, Australia and most other Organisation for Economic Co-operation and Development countries found that the breadth and depth of a credit market was positively associated with the extent of the credit information that was exchanged between lenders.[24] A number of submissions to the ALRC cited the example of Hong Kong, which appears to be experiencing far fewer loan defaults since the introduction of comprehensive credit reporting in 2002, although the ALRC also noted that it was not clear to what extent the change was due to the recovery in Hong Kong's economy that occurred at the same time.[25]

The ALRC identified methodological limitations and assumptions made by the research[26]. For example, the Barron and Staten modelling did not take into account issues such as the weight given to more comprehensive credit information provide by customers under the Australian model, the possibility that the assessment processes used by credit providers may differ from the research models. The research assumed that those credit reporting systems which collected more information used that information effectively. The research did not consider other economic factors, including country specific factors, which may have positively influenced the availability of credit or the impact of any broader economic factors on default levels. In addition, the research was conducted before the Global Financial Crisis.

Australian studies

[22] M Staten and J Barron, *Positive Credit Report Data Improves Loan Decision-Making* (2007) Australian Finance Conference, viewed and cited by the ALRC report at paragraph 55.96.
[23] ALRC Report paragraph 55.97.
[24] T Jappelli and M Pagano, *Information Sharing, Lending and Defaults: Cross-Country Evidence* (2000) Centre for Studies in Economics and Finance, University of Salerno. The Jappelli and Pagano research was referred to in: MasterCard Worldwide, *Submission PR 237,* viewed and cited by the ALRC Report paragraph 55.98.
[25] ALRC Report paragraph 55.103 and 55.104.
[26] ALRC Report paragraph 55.100.

Research measuring the predictive effect of adding additional information to credit reporting databases to assess credit worthiness was conducted at the initiative of the Australian Retail Credit Association (ARCA) and sponsored by a number of credit providers.[27] The research considered a number of models under which additional information was collected. The models considered were identical to the options identified above (see heading 3, Options). Four major Australian banks and a number of international financial services groups participated in the research by analysing their own internal data to estimate the relative predictive effect of different information variables as identified in each option.

The research produced a percentage score to indicate how useful each option was to credit providers in collecting information to assess credit worthiness. The benchmark against which each option was assessed was a hypothetical situation where all relevant credit reporting information (including, for example, full details of repayment performance, which is not a feature of any of the options) was available. This benchmark was assigned a performance score of 100%. When the performance of each option was compared to the benchmark, the research reached the following conclusions:

- Option 1 - the permitted categories of information are unchanged - the predictive value of the information is 10%.
- Option 2(a) - the permitted categories of information are expanded to include the four additional variables – increases the predictive value of the information above option 1 by an additional 23% to a total of 33%.
- Option 2(b) - the permitted categories of information are expanded to include the four additional variables and repayment performance history - increases the predictive value of the information above option 2(a) by an additional 22% to a total of 55%.

However, the research methodology and research results are not available and have not been independently verified. The predictive scores assigned to each option are notional in the sense that they are a comparison against a benchmark that does not currently exist and there is no evidence provided to indicate how the contribution of each information element was assessed. In addition, the benchmark was not recommended by the ALRC, is not an option proposed in this RIS, and has not been proposed or supported by stakeholders, including ARCA, as an appropriate model for Australian conditions.

4.2.2.3 Research on macro-economic benefits

A 2004 study conducted by ACIL Tasman for MasterCard modelled the macro-economic impact of introducing more comprehensive credit reporting in Australia. The report concluded that comprehensive credit reporting would generate a one-off increase in capital productivity of 0.1%, which would translate to economic benefits to the Australian economy of up to $5.3 billion, in net present terms, over the next 10 years.[28] ACIL Tasman used what was described as an 'applied general equilibrium model' of the Australian and world economies to quantify the benefits of more comprehensive credit reporting. In conducting the research, assumptions were made in the model which assumed that more efficient credit markets would have implications for most sectors of the economy.

---

[27] Australasian Retail Credit Association, *Submission to the ALRC*, PR 352, 29 November 2007.

[28] ACIL Tasman, *Comprehensive Credit Reporting: Executive Summary of an Analysis of its Economic Benefits for Australia [prepared for MasterCard International]* (2004), 3. See also ACIL Tasman, *Comprehensive Credit Reporting: Main Report of an Analysis of its Economic Benefits for Australia [Prepared for MasterCard International]* (2004), 28, viewed and cited by the ALRC Report paragraph 55.106 to 55.108.

Research conducted by Access Economics on behalf of Veda Advantage claimed that more credit reporting information would enable lenders to improve the accuracy of risk assessment, reduce defaults and debt over commitment and provide credit to those who cannot currently prove their creditworthiness. Additionally, the research found that comprehensive credit reporting would also lead to an overall increase in consumer debt levels and a related increase in consumer spending. [29]

Advice from Treasury confirmed that comprehensive credit reporting is likely to lead to some small equity and efficiency benefits for credit market participants and the economy more broadly. However, the research is subject to similar criticisms to that made about research on credit market effects. Treasury have advised that the methodologies employed to measure the macro-economic effects have limitations. The ALRC noted that it is difficult to model precisely the macro-economic impact of comprehensive credit reporting due to the level of complexity and the small orders of magnitude involved in assessing the possible benefits. The ALRC drew the following conclusion:

It is questionable whether any modelling will provide definitive answers. For example, Australia is recognised as having a credit market that is very competitive by international standards. This may limit the potential for further competitive gains resulting from more comprehensive reporting. Equally, a macro-economic upturn seems likely to have a much greater influence on credit availability than any change to a credit reporting system.[30]

4.2.2.4 Research on competition in credit markets

The credit reporting industry strongly advocates the view that comprehensive credit reporting will have a positive effect on competition in Australian credit markets. The 2004 ACIL Tasman report stated that, for example, the experience of the US in the 1990s following increases in the types of personal data collected and used in credit reporting saw a 'a wave of new entrants into the bank credit card market'.[31] The benefits of this competition were said to put downward pressure on interest rates and fees for bank credit cards and encourage the targeting of lower interest rates to low risk borrowers. The breadth of the credit card market also expanded. However, the report does not provide evidence to clearly demonstrate the extent to which the identified benefits were directly attributable to credit reporting changes or whether other changes in the consumer credit environment had a significant impact.

In summary, the research suggests greater economic benefits than disadvantages flowing from the introduction of comprehensive credit reporting. The economic benefits are principally found in improving interest rate pricing. The Treasury in its submission to the ALRC noted that overall comprehensive credit reporting would address information asymmetries and thereby improve the targeting of credit, and the assessment, and thus pricing, of risk.[32]

[29] Access Economics (for Veda Advantage), The Benefits of Broadening Access to Credit via Comprehensive Credit Reporting, July 2008

[30] ALRC Report paragraph 55.108.

[31] ACIL Tasman, *Comprehensive Credit Reporting: Executive Summary of an Analysis of its Economic Benefits for Australia [prepared for MasterCard International]* (2004), 3.

[32] Department of Treasury *ALRC Review of Privacy Law Treasury Submission* December 2007

4.2.3 Impact of Option 2(b) - Expand the permitted categories to include four additional categories of personal information (Option 2(a)) with the addition of including an individual's repayment history

Individuals - Benefits

The inclusion of this additional data set will enhance the predictive value of credit worthiness which should lead to more informed lending practices and result in greater efficiency and effectiveness in consumer credit lending.

An enhanced predictive value may lead to improved pricing of credit risk which may provide more affordable credit (through, for example, reduced interest rates or transactions costs) for low risk consumers and greater access to credit for consumers who may not have been able to otherwise demonstrate an adequate credit history. However, the likely benefits to consumers will depend, in part, on the level of competition in the consumer credit market (in the same way that this issue may influence the possible benefits to individuals noted above under Option 2(a)).

Individuals -Costs

Individuals who have poor credit histories may have difficulty in obtaining credit or be required to obtain more costly credit (for example, from providers who lend at higher rates).

As access to this dataset may increase the number of loans issued overall, there may be a risk that there will be an increase in irresponsible lending to those unable to meet their obligations. However, the ALRC recommended repayment history information only be permitted once credit providers are subject to responsible lending obligations.

Individuals who are deemed to be a poor risk based on greater transparency about credit worthiness may find that the face a higher price for access to credit (assuming credit providers introduce differential pricing).

This option also presents similar possible costs to individuals as identified in relation to option 2(a). Permitting additional categories of personal information to be collected, used and disclosed, including the inclusion of an individual's repayment history may increase the risk of data inaccuracy, misuse for marketing or other unauthorised purposes, including identity fraud. Any inaccurate records may create restrict individuals gaining access to credit. Data is not available to quantify the possible cost. If there are no significant changes to the numbers of CRAs operating in Australia, extremely large amounts of data about individuals will be held and maintained by a small number of CRAs which may increase the risk of data security challenges and the consequences of any potential breaches. Information is not available to quantify the possible cost of data inaccuracy. In many instances, the cost to any individual that may be affected by inaccurate records will not be obvious as individuals may resolve the issue by dealing directly with the credit provider or the CRA.

Credit Reporting Agencies - Benefits

The business model and marketability of CRA's will be improved by allowing them to collect, use and disclose a greater amount of data on individuals who apply for credit, in turn giving CRA's the opportunity to sell a more effective product.

Implementing repayment history data at the same time as the other proposed data sets in Option 2(a) would significantly reduce set up costs for credit reporting agencies than if it was decided at a later date to separately implement the repayment history data set.

Credit Reporting Agencies - Costs

As noted under option 2(a), CRAs are likely to incur financial costs associated with developing systems to handle the additional information. However, CRAs can make commercial decisions about how they raise funds to invest in building systems to expand their systems and business operations and how they decide to recoup any investments they chose to make. CRAs may choose to off-set the investment costs against fees obtained from allowing credit providers to access the more comprehensive credit reporting information. For example, they may change their fee structure, market their services to a broader range of credit providers, or develop new services to market to their existing client base of credit providers. CRAs have not provided any information on the commercial decisions they may make to address any costs.

Credit Providers – Benefits

The listing of repayment history would provide credit providers with an independent and easily obtainable source of information about an individual's repayment history and may assist credit providers in identifying individuals who are under credit stress. Access to this information is viewed by credit providers as an important tool to complement any responsible lending obligations.

It is possible that the expected greater efficiencies gained by including repayment history information (in terms of improved credit delinquency predictability, which in turn reduces costs associated with defaulting customers) may offset the administrative costs involved in setting up comprehensive credit reporting under the four datasets in Option 2(a).

The inclusion of the repayment history data set in the credit reporting system at the same time as the other data sets in Option 2(a) will significantly reduce set up costs for credit providers than if it was decided at a later date to separately implement the repayment history data set.

Credit Providers – Costs

As noted under option 2(a), the systems and processes used by credit providers to assess credit applications may change to deal with access to more comprehensive information. If systems and processes change this may result in some costs for credit providers. No information is available to quantify any cost that may occur.

As noted under option 2(a), there may be higher costs to access credit information if CRAs choose to increase fees to off-set the costs of developing their systems. It is not possible to quantify these costs as this will be a commercial decision for CRAs and there is no information available on what choices CRAs may make to recoup any additional costs they may incur in updating their systems.

However, a credit provider would not be required to access comprehensive credit reporting information unless it was deemed necessary for their business and was cost effective. The regulation would simply set up a tool which credit providers could access voluntary.

Small Businesses - Benefits

To the extent that small businesses currently use the credit reporting system, access to repayment history information is expected to allow small businesses to more accurately assess the risks involved in lending to an individual. More information will allow small businesses to avoid lending to those who are over-committed, leading to lower rates of customer indebtedness and defaults.

Small Businesses - Costs

Although there is no information available on the number of small businesses that currently use the credit reporting system, more small businesses may wish to use the credit reporting system in it includes repayment history information. Small businesses may consequently face costs in developing processes to assess credit applications.

There may be higher costs to access credit information if CRAs choose to increase fees to off-set the costs of developing their systems. It is not possible to quantify these costs as this will be a commercial decision for CRAs and there is no information available on what choices CRAs may make to recoup any additional costs they may incur in updating their systems**.**

4.2.3.1 Research specific to the listing of repayment history

As noted above, research by ARCA found that including the repayment history of an individual significantly increased the predicative value of a credit report to 41%. This research accords with widely accepted economic theory that making more information available to credit providers will tend to increase efficiency in the market for credit. It will also assist in making credit more available to those able to repay and reduce rates of default (or both). There was no significant disagreement among stakeholders in their submissions to the ALRC Report that more comprehensive credit reporting has the potential to improve risk assessment by credit providers, even among those who expressed concern about how this improved risk assessment would be used in the credit market.

There is little evidence to demonstrate that this additional data set will subject consumers to greater burdens in terms of higher priced credit or lack of credit. Such matters will be dependent on the applicable business practices of the credit provider and the need to adequately price credit in terms of a person's risk. It is noted that in many circumstances the number 'bad risk' customers who are denied credit will effectively be balanced by those 'good risk' customers who are afforded credit under the comprehensive scheme (but would not have been under the 'negative scheme).

It should be noted that Option 2(b) is only to be implemented with the implementation of responsible lending legislation under the NCCP Bill. While the benefit that repayment history would provide credit providers in determining credit risk of individuals, there are strong concerns expressed by privacy and consumer advocates that this extra category of information does not necessarily guarantee responsible lending of credit. Advocates are concerned that the repayment history will provide credit providers with a very clear picture of a person's financial status without imposing any obligations to use this information in a responsible way. Consumer advocates in particular consider that the availability of more credit information will lead to less risk adverse decisions by credit providers (i.e. credit providers will use a good repayment history to justify providing credit to an individual even where the individual has credit burdens beyond their means). There is therefore a clear link between potential regulation imposing responsible lending obligations and the possible implementation of comprehensive credit reporting.

These concerns would be off-set by the requirement that only those credit providers that are subject to the responsible lending requirements in the NCCP Bill would be allowed to access repayment history from CRAs.

To offset privacy concerns the ALRC made recommendations that require credit providers and CRAs to enhance data quality and security requirements and provide for more effective complaint handling procedures. Chapter 58 and 59 of the ALRC Report outlines a series of recommendations regarding these matters. Recommendation 58-4 recommended that CRAs

should be required to enter into agreements with credit providers to ensure the quality and security of data and to implement controls to ensure data is accurate, complete and up to date. Recommendation 58-7 provides that credit providers may only list overdue payment or repayment performance history where the credit provider is a member of an external dispute resolution scheme recognised by the Privacy Commissioner. Additionally recommendation 59-8 requires that evidence must be provided to an individual substantiating information in a credit report within 30 days where the credit reporting information is disputed or alternatively the matter must be referred to an external dispute resolution scheme recognised by the Privacy Commissioner.

5 Consultation

5.1 ALRC Report Consultation

The ALRC consulted with a wide variety of stakeholders which included CRAs, credit providers, consumer and privacy advocates and the OPC. The ALRC found there was broad support for the implementation of some form of more comprehensive reporting, especially from CRAs and credit providers.[33]

Consumer groups, privacy advocates, the OPC and the Banking and Financial Ombudsman generally opposed more comprehensive credit reporting. These stakeholders focused on alternatives and desirable pre-conditions to the possible introduction of more comprehensive credit reporting.[34]

A number of stakeholders, including OPC, suggested that further study is required before reaching any decision to recommend the implementation of more comprehensive credit reporting, including studies which focus on the possible impact on over-indebtedness and access to affordable credit. A CRA had proposed to the ALRC that it would conduct a further study to model the effect that more comprehensive consumer credit reporting would have on the accuracy of credit providers' application risk evaluation. However, the study was not carried out, in part because of what the CRA believed to be existing restrictions under the Privacy Act.[35]

5.2 Consultation since the release of the ALRC Report

The Government undertook extensive consultations with, and received written submissions from, relevant stakeholders on the ALRC's credit reporting recommendations. Stakeholders identified included CRAs, credit providers, relevant industry and professional organisations, academics, and consumer and privacy advocates and organisations. The Government also publicised the consultations and opened them to submissions from the public.[36]

The Government held a number of roundtable consultations on the ALRC credit reporting recommendations in December 2008. There were 22 credit reporting industry attendees and eight privacy and consumer advocate attendees. 15 written submissions were received from the stakeholders. The Department also held a number of individual meetings with stakeholders in the first half of 2009 to discuss the application of the ALRC's recommendations.

There was broad support for the introduction of more comprehensive credit reporting. While some consumer and privacy advocates remained opposed to the ALRC's recommendations for more comprehensive credit reporting, most consumer and privacy advocates reluctantly

[33] ALRC Report paragraph 55.115
[34] ALRC Report paragraph 55.133
[35] ALRC Report paragraph 55.125
[36] http://www.smos.gov.au/media/2008/mr_372008.html viewed 2 September 2009.

agreed with many of the recommendations and the inclusion of repayment performance history. Those who agreed with the ALRC recommendations only supported comprehensive credit reporting to the extent that it was introduced strictly along the lines recommended by the ALRC Report. CRAs and large credit providers vigorously supported the inclusion of repayment history and strongly expressed their view that they considered this dataset to be the decisive factor in improving the credit reporting system. CRAs and credit providers expressed the view that the absence of repayment history would be likely to mean that the benefits of comprehensive credit reform would not outweigh the costs of introducing the other changes.

6 Conclusion and Recommended Option

Option 2(b) is preferred. The introduction of more comprehensive credit reporting in the form of the additional five data sets will provide consumer credit providers with the opportunity to access enhanced information to establish an individual's credit worthiness. It is expected that this will allow more robust assessments of consumer credit risk, both in the market as a whole and in relation to individual applications, which can assist responsible lending and potentially lead to lower consumer credit default rates. The economic benefits to industry and individuals alike outweigh the reduction of privacy protections to these categories of personal information. However, the extent to which consumers gain will depend, in part, on the level of competition in the consumer credit market. The inclusion of repayment history information appears to provide an appropriate increase in the predictive value of credit reporting information. Recognising the importance of this information to the ability of credit providers to make responsible lending decisions, the Government has decided to implement responsible lending obligations in the NCCP Bill.

7 Implementation and Review

The Government will consider the public release of the stage one Government response to the ALRC Report, which includes the ALRC's credit reporting recommendations. The Government intends to implement the Government's response to the ALRC recommendations through draft legislation which will be released for public comment. In relation to the credit reporting provisions of the draft legislation, it is anticipated that further consultations will occur with a small number of identified expert stakeholders to obtain their assistance in addressing technical issues to be covered by the drafting process. As part of this process transitional issues will be considered, which will include any necessary transitional arrangements to assist in minimising any possible negative effects to the consumer credit market from the implementation of the credit reporting reforms.

The Government has released the NCCP Bill for public comment and made announcements indicating the Government's commitment to introduce responsible lending obligations. This is consistent with the terms of ALRC recommendation 55-3, which recommended repayment history information only be made available if the Government is satisfied there is an adequate framework imposing responsible lending obligations.

ALRC recommendation 55-5 stated that the more comprehensive credit reporting information should be deleted two years after the date on which a credit account is closed. The Government will include timeframes for the deletion of information in the implementation of the Government's response to the credit reporting recommendations.

It is recommended that a review of the introduction of the additional datasets by the Government take place in five years from the commencement of more comprehensive credit reporting in accordance with Recommendation 54–8 of the ALRC Report.

PART B: Industry Developed Credit Reporting Code of Conduct

8. Problem

Non-legislative guidance should be issued to deal with a range of operational matters to ensure effective compliance with the requirements of the credit reporting provisions of the Privacy Act. The appropriate form of this guidance is the issue to be determined.

Section 18A of the Privacy Act currently requires the Privacy Commissioner to issue a Code of Conduct dealing with operational matters. The Privacy Act sets out high level obligations and does not deal with detailed operational matters. In addition, the Privacy Act does not prescribe detailed operational procedures because it would not be a flexible mechanism to deal with issues of detail. For example, it would be difficult to take into account changing technical standards and practices that may occur in the credit reporting industry and which may require the revision of the detailed guidance material.

In recommendation 54-9 the ALRC proposes that CRAs and credit providers develop an industry Code of Conduct in consultation with consumer groups and regulators. The ALRC expressed the view that an industry developed Code would form a necessary adjunct to the credit reporting provisions in the Privacy Act. The ALRC recommended that the Code be developed by industry because of the perceived need for industry to have a greater involvement in developing procedures which affect their day to day compliance with the Privacy Act.

Consistent with ALRC recommendation 48-1 on binding codes, the credit reporting Code would 'fill in the gaps' between the new credit reporting provisions and compliance with the obligations set out in the provisions. It would provide detailed guidance within the framework of the requirements of the credit reporting provisions in the Privacy Act.

In assessing the suitability of the type and structure of a credit reporting Code, it should be noted that the details of the Code's content can only be developed once the Government has settled the framework of the new credit reporting system. However, it is expected that the Code would be an appropriate mechanism to address the following matters:

- procedures for reporting repayment performance history
- data quality procedures to ensure consistency and accuracy of credit reporting information, such as:
    - the timeliness of the reporting of credit reporting information;
    - rules on the calculation of overdue payments for credit reporting purposes;
    - obligations to prevent the multiple listing of the same debt;
    - requirements to update credit reporting information; and
    - rules around linking credit reporting records which may or may not relate to the same individual
- dispute resolution processes, and
- protocols and procedures for the auditing of credit reporting information.

9. Objectives

The objective of government action is to respond to the ALRC recommendations on the introduction of an industry led Code of Conduct in the context of the Government's response to the ALRC recommendations on the credit reporting system and the wider ALRC review of privacy law. The specific objective is to provide a mechanism to put into place standards

dealing with operational issues to assist compliance by credit reporting industry with the requirements of the new credit reporting system.

10. Options that may achieve the objectives

10.1 *Implementation scope*

The jurisdiction of the Privacy Act sets the scope for implementing a credit reporting Code of Conduct. Within this framework, the parameters of the proposed options are confined to responding to the ALRC Report's recommendations on a credit reporting Code.

10.2 *Option 1 – Maintain the present Credit Reporting Code of Conduct process*

This option would preserve the existing requirement for the Privacy Commissioner to issue a credit reporting Code of Conduct. The existing Code of Conduct will require revision to deal with operational issues raised by more comprehensive credit reporting (if accepted).

10.3 *Option 2 – Introduce a binding Code of Conduct developed by industry in accordance with the code making powers set out in Part IIIAA of the Privacy Act*

Under this option:

- the Privacy Act would specifically require CRAs and credit providers to develop a Code covering a broad range of operational issues as identified in the Privacy Act and in consultation with consumer representatives and regulators
- any CRA or credit provider who intended to participate in the consumer credit reporting industry would be required to be a party to the Code
- the Code would be a legally binding Code under the Privacy Act. It would operate in addition to the credit reporting provisions and could not override or apply lesser standards than those contained in the Privacy Act
- the Code must be approved by the Privacy Commissioner, who would also have the power to review the Code; and
- a breach of the Code would be deemed to be a breach of the Privacy Act and the Privacy Commissioner or a relevant External Dispute Resolution (EDR) scheme would be entitled to determine a complaint in accordance with the provisions of the Privacy Act or Code (as appropriate).

The industry may choose to address some credit reporting issues (such as reciprocity between industry participants in the credit reporting system) which will not be regulated by the credit reporting provisions. It would be a matter for industry to determine what, if any, additional issues should be included. As these matters would fall outside the credit reporting provisions they would not require approval by the Privacy Commissioner.

10.4 *Option 3 – Permit a non-prescribed voluntary industry Code of Conduct*

Under this Option:

- the Privacy Act would not set out any requirements for the existence or contents of a Code of Conduct
- the Code would not be binding under the Privacy Act
- it would be a matter for the credit reporting industry to determine whether to develop a Code and the contents of the Code

- any Code developed by industry would be a non-prescribed voluntary industry code of conduct under the *Trade Practices Act 1974*. Depending on the contents of the Code, it may be authorised by the Australian Competition and Consumer Commission (ACCC) for certain conduct on public benefit grounds that may otherwise be proscribed by the Trade Practices Act
- Any Code would establish standards which would be voluntarily agreed by its signatories. The Code would be a contractual arrangement; and
- the Code would be enforceable where CRAs and credit providers have agreed to be bound by the Code and established dispute resolution procedures in the Code (such as an EDR service). The terms of the Code would not be enforceable by the Privacy Commissioner or the ACCC.

11. Assessment of impacts

11.1 *Impact group identification*

The groups affected by the Options, in the order of the magnitude of the impact, are:

- CRAs
- Credit Providers
- OPC
- Small businesses; and
- Individuals.

11.2 *Assessment of costs and benefits*

11.2.1 Impact of Option 1 – maintain the present Code of Conduct process

Credit Reporting Agencies – Benefits

While the existing Code would need to be revised if more comprehensive credit reporting is introduced, it is likely there would be minimal costs in complying with a revised Code. CRAs would be consulted in the development of the Code to ensure business practices are adequately considered. To the extent that CRAs decide to collect more comprehensive credit reporting information, compliance with the revised Code could be built into the development of any new systems and procedures required by the adoption of more comprehensive credit reporting. Where existing requirements of the Code are unchanged, there would be no compliance costs as CRAs would already be in compliance with these requirements.

Credit Reporting Agencies – Costs

The current Code of Conduct does not deal in detail with some of the operational and procedural steps used within existing industry practices, which may lead to less clarity and consistency within the industry. Further detail could provide more precise guidance to CRAs on current industry practices, assisting CRAs to comply with the credit reporting provisions.

While CRAs would be consulted by the OPC in any Code revision process resulting from the reforms to the credit reporting provisions, they would not have a central role in amendments to the Code of Conduct. This reduces the ability of CRAs to form and direct changes in the Code of Conduct, such as in situations where technological developments may mean changes to operational practices that could benefit from guidance in the Code of Conduct. CRAs would not be able to take the initiative in developing and proposing revisions to the Code, but instead would need to convince the OPC to initiate a review of the Code. A lack of clear

guidance may restrict future developments in the industry, which may result from the adoption of new technologies or the identification of new opportunities to use or manage data. This may have the cost of reducing possible economic opportunities and benefits. Evidence is not available to quantify any possible costs.

The purpose of the Code is to provide practical guidance to CRAs to assist compliance with the requirements of the Privacy Act and it is expected that detailed compliance information will be of significant assistance to the CRA industry. However, there is a slight possibility that the existence of the Code may discourage new CRA industry entrants. New entrants may prefer to establish alternative procedures and processes that comply with the requirements of the Privacy Act but do not match the detailed guidance contained in the Code. In addition, new entrants would not have had the opportunity to contribute to the Code development process.

Credit Providers – Benefits

While the existing Code would need to be revised if more comprehensive credit reporting is introduced, it is likely there would be minimal costs in complying with a revised Code. Credit providers would be consulted in the development of the Code to ensure business practices are adequately considered. Compliance with the revised Code could be built into the development of any new systems and procedures required by the adoption of more comprehensive credit reporting. Where other existing requirements of the Code are unchanged, there would be no compliance costs as credit providers would already be in compliance with these requirements.

Credit Providers – Costs

Similar issues exist for credit providers as those identified for CRAs. The current Code of Conduct does not deal in detail with some of the operational and procedural steps used within existing industry practices, which may lead to less clarity and consistency within the industry. Further detail could provide more precise guidance to credit providers on current industry practices, assisting credit providers to comply with the credit reporting provisions.

Credit providers would not have a central role in amendments to the Code of Conduct, although they would be consulted by the OPC in any Code revision process resulting from the reforms to the credit reporting provisions. This reduces the ability of credit providers to form and direct changes in the Code of Conduct, such as in situations where technological developments may mean changes to operational practices that could benefit from guidance in the Code of Conduct. The credit industry would not be able to take the initiative in developing and proposing revisions to the Code, but instead would need to convince the OPC to initiate a review of the Code. A lack of clear guidance may restrict future developments in the industry, which may result from the adoption of new technologies or the identification of new opportunities to use or manage data. This may have the cost of reducing possible economic opportunities and benefits. Evidence is not available to quantify any possible costs.

The purpose of the Code is to provide practical guidance to credit providers to assist compliance with the requirements of the Privacy Act and it is expected that detailed compliance information will be of significant assistance to credit providers. However, there is a slight possibility that the existence of the Code may discourage new credit providers. New credit providers may prefer to establish alternative procedures and processes that comply with the requirements of the Privacy Act but do not match the detailed guidance contained in the Code. In addition, new credit providers would not have had the opportunity to contribute to the Code development process.

Office of the Privacy Commissioner – Benefits

This option would ensure that OPC retains complete control over the development and promulgation of the Code. OPC would continue to be required to consult with stakeholders in revising the Code, but it would be a matter for OPC to decide when to review the Code and what elements of the Code require revision.

Office of the Privacy Commissioner – Costs

The OPC does not have the necessary industry knowledge to provide specific guidelines on operational and procedural issues. While the OPC is required to consult stakeholders and can obtain extensive information through the consultation process, the OPC would be required to devote resources to reviewing the Code and developing amendments. The proposed introduction of more comprehensive credit reporting means that the OPC will be required to review the Code. It is not possible to estimate the total expected cost of a full review of the Code and there have been no comprehensive reviews of the Code on which to base estimates of possible costs.

Small Businesses – Benefits

Some small businesses may be credit providers depending on whether they offer goods or services on terms that involve credit. It would be expected that any review of the Code by the OPC would include consultation with small business representatives as stakeholders in the review. Businesses are not required to participate in the credit reporting system and, where small businesses chose not to do so, they would not be affected by a revised Code.

Small Businesses - Costs

A revised Code will deal in detail with operational matters arising from the adoption of more comprehensive credit reporting. To the extent that small businesses decide to participate in the credit reporting system and use more comprehensive credit reporting information, they will need to comply with the requirements of the Code, including, for example, requirements to participate in EDR services. It is not possible to quantify the possible compliance costs for small businesses as there is no information available on the number of small businesses likely to use more comprehensive credit reporting.

Individuals – Benefits

Individuals would benefit from consistent operational standards for industry practices. Individuals would be concerned to ensure that the Code achieved an appropriate balance between the protection of personal information and the operational needs of the credit reporting industry. As the OPC has responsibility for the development and review of the Code, individuals can rely on the OPC to ensure their interests in the effective protection of personal information are protected.

Individuals would also benefit from the legal status of the Code to ensure their rights are enforced. The Code would remain a disallowable instrument, which means that a breach of the Code could be the subject of a complaint to the Privacy Commissioner**.**

Individuals – Costs

A Code is intended to ensure consistency and certainty in operational practices throughout the credit reporting industry. There are no obvious costs for individuals.

11.2.2 Impact of Option 2 – Introduce a binding Code developed by industry in accordance with the code making powers set out in Part IIIAA of the Privacy Act

Credit Reporting Agencies – Benefits

This option requires the credit reporting industry to develop a Code that would be binding under the Privacy Act. Credit industry control of the code making process would:

- allow the industry to apply detailed knowledge of industry practices to determine the best procedures to ensure practical compliance with the requirements of the Privacy Act
- provide the industry with the flexibility to review the Code and develop necessary changes to the Code (subject to OPC approval) as required by changes in industry standards; and
- ensure the credit reporting industry adopts best standard practices which have been developed in consultation with all industry participants, improving the overall reliability of industry practices and enhancing the operation of the credit reporting system.

The ability of the credit reporting industry to develop (in consultation with stakeholders, including consumer advocates) and adhere to a binding Code may assist the industry build greater trust by individuals in the operational standards and reliability of credit reporting practices**.**

Credit Reporting Agencies – Costs

The code making process would require the cooperation of all industry participants to develop specific operational and procedural requirements. The process of developing the Code may involve costs to the industry, such as:

- the time taken to develop a binding Code may be significant as industry groups must come to agreement about the provisions of the Code and take into account that the OPC will also need time to approve the Code
- costs associated with drafting the Code
- costs involved in consulting with stakeholders, both within the credit industry as well as with consumer and privacy advocates and regulators; and
- possible costs associated with any future review of the Code.

It is not possible to estimate the actual costs that may be incurred. Many of these potential costs are unlikely to be incurred because the credit industry has already begun work on the development of a Code. The Australian Retail Credit Association (ARCA) is developing a draft Code on a range of operational matters that could be readily modified to include additional matters raised by the introduction of more comprehensive credit reporting. The ARCA Code is discussed below in section 11.2.4.

It is expected that detailed compliance information will be of significant assistance to the CRA industry. However, there is a slight possibility that the existence of the Code may discourage new CRA industry entrants. New entrants may prefer to establish alternative procedures and processes that comply with the requirements of the Privacy Act but do not match the detailed guidance contained in the Code. In addition, new entrants would not have had the opportunity to contribute to the Code development process.

Credit Providers – Benefits

This option requires the credit reporting industry to develop a Code that would be binding under the Privacy Act. Credit industry control of the code making process would:

- allow the industry to apply detailed knowledge of industry practices to determine the best procedures to ensure practical compliance with the requirements of the Privacy Act
- provide the industry with the flexibility to review the Code and develop necessary changes to the Code (subject to OPC approval) as required by changes in industry standards; and
- ensure the credit reporting industry adopts best standard practices which have been developed in consultation with all industry participants, improving the overall reliability of industry practices and enhancing the operation of the credit reporting system.

The ability of the credit reporting industry to develop (in consultation with stakeholders, including consumer advocates) and adhere to a binding Code may assist the industry build greater trust by individuals in the operational standards and reliability of credit reporting practices.

Credit Providers – Costs

The code making process would require the cooperation of all industry participants to develop specific operational and procedural requirements. The process of developing the Code may involve costs to the industry, such as:

- the time taken to develop a binding Code may be significant as industry groups must come to agreement about the provisions of the Code and take into account that the OPC will also need time to approve the Code
- costs associated with drafting the Code
- costs involved in consulting with stakeholders, both within the credit industry as well as with consumer and privacy advocates and regulators; and
- possible costs associated with any future review of the Code.

It is not possible to estimate the actual costs that may be incurred. Many of these potential costs are unlikely to be incurred because the credit industry has already begun work on the development of a Code. The Australian Retail Credit Association (ARCA) is developing a draft Code on a range of operational matters that could be readily modified to include additional matters raised by the introduction of more comprehensive credit reporting. The ARCA Code is discussed below in section 11.2.4. However, ARCA appears to represent large organisations in the credit industry. If ARCA takes a leading role in developing the Code, it is possible that smaller credit providers which are not members of ARCA may not be in a position to influence the code making process to the same extent as ARCA members. This may mean, for example, that industry practices which suit larger organisations are incorporated into the Code as industry standards, disadvantaging smaller industry participants that do not use the same practices.

The purpose of the Code is to provide practical guidance to credit providers to assist compliance with the requirements of the Privacy Act and it is expected that detailed compliance information will be of significant assistance to credit providers. However, there is a slight possibility that the existence of the Code may discourage new credit providers.

New credit providers may prefer to establish alternative procedures and processes that comply with the requirements of the Privacy Act but do not match the detailed guidance contained in the Code. In addition, new credit providers would not have had the opportunity to contribute to the Code development process.

Office of the Privacy Commissioner – Benefits

A Code would create certainty for the OPC that a breach of the Code is a breach of the Privacy Act and it would also provide the OPC with industry standards by which to apply the credit reporting provisions. Industry standards would give greater clarity about the application of the Act to the industry and should result in more efficient complaint resolution, resulting in less confusion as to whether a breach of the code is an interference with privacy. Approval from the OPC would ensure the OPC is satisfied with industry's interpretation of the credit reporting provisions.

Office of the Privacy Commissioner – Costs

It is expected that the OPC would face minimal costs when compared with Option 1. The OPC would not face costs in the development of the Code, but would be required to incur some costs in approving the Code. It is not possible to estimate the costs of approving the Code until a draft Code is developed.

Small Businesses – Benefits

Some small businesses may be credit providers depending on whether they offer goods or services on terms that involve credit. In the development of a Code the credit reporting industry would be required to consult with affected stakeholders. It is expected that this consultation process would include a mechanism for small businesses to contribute to the development of the Code, including through consultation with representative organisations. As the Code would require authorisation by the OPC, it would be expected that the OPC would consider whether effective consultation had occurred, including with small business stakeholders. Businesses are not required to participate in the credit reporting system and, where small businesses chose not to do so, they would not be affected by a Code**.**

Small Businesses - Costs

A Code will deal in detail with operational matters arising from the adoption of more comprehensive credit reporting. To the extent that small businesses decide to participate in the credit reporting system and use more comprehensive credit reporting information, they will need to comply with the requirements of the Code, including, for example, requirements to participate in EDR services. It is not possible to quantify the possible compliance costs for small businesses as there is no information available on the number of small businesses likely to use more comprehensive credit reporting.

Individuals – Benefits

Complaints by individuals would be subject to a clear EDR process. As the Code would be enforceable by the OPC, adherence with the Code to the protection of individual's privacy would be stronger as a breach of the Code would be a breach of the Privacy Act.

Individuals would benefit from consistent operational standards for industry practices. Individuals would be concerned to ensure that the Code achieved an appropriate balance between the protection of personal information and the operational needs of the credit reporting industry. As the OPC has responsibility for the development and review of the Code, individuals can rely on the OPC to ensure their interests in the effective protection of personal information are protected.

Individuals would also benefit from the legal status of the Code to ensure their rights are enforced. The Code would remain a disallowable instrument, which means that a breach of the Code could be the subject of a complaint to the Privacy Commissioner.

Individuals – Costs

A Code is intended to ensure consistency and certainty in operational practices throughout the credit reporting industry. There are no obvious costs for individuals**.**

11.2.3 Impact of Option 3 - Introduce a voluntary Code developed by industry

Credit Reporting Agencies – Benefits

This option would not require the credit reporting industry to develop a voluntary Code. It would be a matter for the industry to decide whether or not to develop a voluntary Code. Any costs involved in the development of a Code would not be imposed by regulation but subject to commercial decisions about the costs and benefits by the industry.

If the credit reporting industry chooses to develop a voluntary Code, the industry would remain in control of the development process. Industry control over the code making process would:

- allow the industry to apply detailed knowledge of industry practices to determine the best procedures to ensure practical compliance with the requirements of the Privacy Act
- provide the industry with the flexibility to review the voluntary Code and develop necessary changes as required by changes in industry standards; and
- allow the credit reporting industry to determine whether it needed to adopt standard practices.

A voluntary Code would not require approval from the OPC, potentially reducing costs and delays in implementation. However, approval from the ACCC may be required depending on whether the Code required consideration under the Trade Practices Act.

A voluntary Code would not impede new CRAs entering the market as it would be a commercial decision whether or not the new CRA subscribed to the voluntary Code.

The ability of the credit reporting industry to develop and adhere to a voluntary Code may assist the industry build greater trust by individuals in the operational standards and reliability of credit reporting practices.

Credit Reporting Agencies – Costs

The code making process would require industry cooperation to develop specific operational and procedural requirements. This is expected to involve costs to the industry in the preparation of the voluntary Code, including a cost to develop and draft the voluntary Code. However, ARCA has already drafted a Code and it is expected that the Code could be readily modified to form the basis of the voluntary Code, substantially reducing any costs in the development of a voluntary Code.

A voluntary Code would be required to comply with the ACCC's guidelines for developing effective voluntary industry codes of conduct. The voluntary Code may also require authorisation by the ACCC if it contravenes a provision of the Trades Practices Act, which may extend the time required to develop the voluntary Code.

CRAs would not be required to be members of the voluntary Code. This may lead to inconsistencies in the credit reporting system in ensuring common compliance with the credit reporting provisions.

A voluntary Code would not be enforceable by the OPC. This may be seen by stakeholders (including consumers) as undermining the reliability of the voluntary Code and the enforceability of any consumer rights or industry obligations imposed by the voluntary Code. This may detract from stakeholder trust in the reliability of the credit reporting system.

It is unlikely that the existence of the voluntary Code would discourage new CRA industry entrants. As it will be voluntary, new industry entrants would retain the discretion of not participating in the voluntary Code. They would be able to establish their own alternative procedures and processes that comply with the requirements of the Privacy Act but do not match the detailed guidance contained in the voluntary Code.

Credit Providers – Benefits

This option would not require the credit reporting industry to develop a voluntary Code. It would be a matter for the industry to decide whether or not to develop a voluntary Code. Any costs involved in the development of a Code would not be imposed by regulation but subject to commercial decisions about the costs and benefits by the industry.

If the credit reporting industry chooses to develop a voluntary Code, the industry would remain in control of the development process. Industry control over the code making process would:

- allow the industry to apply detailed knowledge of industry practices to determine the best procedures to ensure practical compliance with the requirements of the Privacy Act
- provide the industry with the flexibility to review the voluntary Code and develop necessary changes as required by changes in industry standards; and
- allow the credit reporting industry to determine whether it needed to adopt standard practices**.**

A voluntary Code would not require approval from the OPC, potentially reducing costs and delays in implementation. However, approval from the ACCC may be required depending on whether the Code required consideration under the Trade Practices Act.

A voluntary Code would not impede new credit providers entering the market as it would be a commercial decision whether or not the credit provider subscribed to the voluntary Code.

The ability of the credit reporting industry to develop and adhere to a voluntary Code may assist the industry build greater trust by individuals in the operational standards and reliability of credit reporting practices.

Credit Providers – Costs

The code making process would require industry cooperation to develop specific operational and procedural requirements. This is expected to involve costs to the industry in the preparation of the voluntary Code, including a cost to develop and draft the voluntary Code. However, ARCA has already drafted a Code and it is expected that the Code could be readily modified to form the basis of the voluntary Code, substantially reducing any costs in the development of a voluntary Code.

A voluntary Code would be required to comply with the ACCC's guidelines for developing effective voluntary industry codes of conduct. The voluntary Code may also require

authorisation by the ACCC if it contravenes a provision of the Trades Practices Act, which may extend the time required to develop the voluntary Code.

Credit providers would not be required to be members of the voluntary Code. This may lead to inconsistencies in the credit reporting system in ensuring common compliance with the credit reporting provisions.

A voluntary Code would not be enforceable by the OPC. This may be seen by stakeholders (including consumers) as undermining the reliability of the voluntary Code and the enforceability of any consumer rights or industry obligations imposed by the voluntary Code. This may detract from stakeholder trust in the reliability of the credit reporting system.

It is unlikely that the existence of the voluntary Code would discourage new consumer credit industry entrants. As it will be voluntary, new industry entrants would retain the discretion of not participating in the voluntary Code. They would be able to establish their own alternative procedures and processes that comply with the requirements of the Privacy Act but do not match the detailed guidance contained in the voluntary Code.

Office of the Privacy Commissioner – Benefits

The OPC would face minimal, if any, costs when compared with Option 1. The OPC would not have a role in the voluntary Code making process, although the industry may choose to consult the OPC for guidance, and the OPC would not have a role in reviewing or authorising the voluntary Code. In any enforcement actions the OPC would not need to consult the voluntary Code in interpreting the credit reporting provisions.

Office of the Privacy Commissioner – Costs

The OPC would not have control over directing the credit reporting industry to develop a voluntary Code or the content of the voluntary Code. As the development of a voluntary Code would not be linked to the Privacy Act, the OPC would not be able to interpret specific credit reporting provisions by referring to the voluntary Code for practical assistance. This may lead to a fragmented approach to the operation of the credit reporting provisions, which may result in increased enforcement costs for the OPC, particularly if individual consumer complaints increased. It may also lead to increased business education costs for the OPC if it was necessary to encourage and educate the industry to ensure greater compliance with the requirements of the credit reporting provisions. It is not possible to quantify these potential costs as they would depend on the nature and severity of any problems which may be encountered.

Small Businesses – Benefits

Some small businesses may be credit providers depending on whether they offer goods or services on terms that involve credit. Businesses are not required to participate in the credit reporting system and, where small businesses chose not to do so, they would not be affected by a voluntary Code. Where small businesses choose to participate in the credit reporting system, participation in the development and implementation of a voluntary Code would provide them with greater certainty about the operation of the system and may increase consumer trust in their compliance with the credit reporting provisions.

Small Businesses - Costs

A voluntary Code would deal in detail with operational matters arising from the adoption of more comprehensive credit reporting. To the extent that small businesses decide to participate in the credit reporting system and use more comprehensive credit reporting information, they would need to consider complying with the requirements of the voluntary

Code. It is not possible to quantify the possible compliance costs for small businesses as there is no information available on the number of small businesses likely to use more comprehensive credit reporting**.**

Individuals – Benefits

Individuals would benefit from consistency in the type of practices engaged in by credit reporting industry participants. Development of a voluntary Code would provide consumer certainty around the practices of participating industry members.

Individuals – Costs

A voluntary Code may not build consumer trust in the practices of the industry or the dispute resolution procedures. Breaches of the voluntary Code would not be enforceable by the OPC. If the voluntary Code requires authorisation by the ACCC, there may be consumer confusion around the appropriate regulator for dispute resolution. It may be the case that not all CRAs or credit providers participate in the voluntary Code, which may create inconsistency and uncertainty for individuals in their dealings with the industry and in resolving consumer complaints.

11.2.4 Further notes relevant to Options 2 and 3: the ARCA Code

ARCA is currently preparing an industry Code to provide safeguards for business-to-business transactions involving consumer credit information. Amongst other matters, the industry Code is intended to regulate the operational processes by which credit providers receive data from CRAs, as well as provide requirements for how credit providers deal with customers on credit reporting issues. The current members of ARCA are ABACUS (Australian Building and Credit Union Societies, known as Australian Mutuals), American Express, ANZ Bank, Bank of Queensland, Bank of Western Australia, Citibank, Commonwealth Bank of Australia, GE Money, HBOS Australia, HSBC Bank, National Australia Bank, St George Bank, Telecom New Zealand, Westpac Bank, Dun and Bradstreet, and Veda Advantage.

ARCA has released a draft Credit Reporting Code of Conduct (the ARCA Code) which it has prepared as a voluntary contractual Code between members along the lines outlined in Option 3. However, the draft ARCA Code provides that membership is mandatory for any CRA with operations in Australian and for any credit provider who wishes to use or disclose credit reporting information. The ARCA Code would require all CRAs to ensure that organisations that seek access to credit reporting information are signatories to the Code or are otherwise bound by the Code provisions (e.g. via contract or terms and conditions of access). It would also allow regulators to require organisations to be bound by the Code (for example as a condition of obtaining a licence).

ARCA's work in developing a Code on behalf of the industry means that much of the work required to create a code has been commenced satisfied. ARCA has undertaken a consultation process and invited submissions from interested parties in April 2009. It is understood that ARCA is currently in the process of considering those submissions and revising the draft Code. Whether the ARCA Code forms the basis for a voluntary Code under Option 3 or a binding Code under Option 2, the document would need to undergo an approval process by the appropriate regulator (the ACCC for Option 3 or the OPC for Option 2).

12 Consultation

12.1 ALRC Report Consultation

The ALRC consulted with a wide variety of stakeholders which included CRAs, credit providers, consumer advocates and the OPC. There was broad support for the implementation of a new credit reporting code. CRAs and the representative body ARCA were strongly in favour of a new code, and as already demonstrated, ARCA is preparing a draft credit reporting code. The OPC was also in favour of a new code. In terms of legislative design, in their submissions to the ALRC, the CRAs and ARCA originally supported a binding code under Part IIIAA as outlined in Option 2.

Consumer groups and privacy advocates generally favoured a binding code approved by the Privacy Commissioner. Matters which were of high importance for these groups were to ensure greater certainty about data accuracy, security and appropriate EDR procedures and processes.

12.2 Consultation since the release of the ALRC Report

The Government undertook extensive consultations with, and received written submissions from, both the credit reporting industry and advocates on the credit reporting recommendations.

The Government held the public roundtable consultations in December 2008. There were 22 credit reporting industry attendees and eight privacy and consumer advocate attendees. 15 written submissions were received from the stakeholders. The Department also held a large number of one-on-one meetings with stakeholders in the first half of 2009 to discuss the application of the ALRC's recommendations.

The views of privacy and consumer advocates remained largely unchanged since the publication of the ALRC Report, and they reinforced their support for a mandatory credit reporting code approved by the OPC. One large credit provider similarly stressed that there should be only one regulator responsible for enforcement of the code.

The position of ARCA and CRAs in relation to the design of a code changed from their original submission to the ALRC. They have submitted that that code should not be binding under the Privacy Act as under Option 2 and favour instead the adoption of a contractual code similar to Option 3.

13 Conclusion and Recommended Option

Option 2 is preferred. Unlike Option 1, Option 2 provides the consumer credit industry with sufficient flexibility and discretion to ensure that the requirements of the Code adequately address industry practice, while at the same time providing the Privacy Commissioner with the power to determine (through the approval process) whether the Code is consistent and compliant with the requirements of the Privacy Act. Option 2 provides for a legally binding Code, which will allow the Privacy Commissioner to ensure an appropriate balance between the privacy needs of individuals and the operational needs of the consumer credit industry. This is not available under Option 3. The requirement under Option 2 for any organisation which wants to participate in the credit reporting system to be a member of the binding Code will ensure consistency in practices across the consumer credit industry. Furthermore, a binding code under the jurisdiction of the Privacy Act (in contrast to a contractual code under Option 3) allows the OPC to interpret specific credit reporting provisions with reference to the Code. This will aid in efficient and consistent complaint resolution for individuals, whether the complaints deal with matters regulated directly by the Privacy Act or by the Code. In addition, the likely costs for industry in complying with a Code developed under

Option 2 are expected to be reduced. The consumer credit industry has already developed and complies with the ARCA Code, which it is expected would form the basis for the new industry developed Code of Conduct under Option 2. The use of the ARCA Code is also likely to reduce the costs to industry in developing a voluntary Code under Option 3. However, the voluntary Code would not be binding on industry and would not establish the same level of certainty around industry practices and consumer complaint resolution procedures as an industry developed Code under Option 2.

14. Implementation and Review

The Government will release a public response to the ALRC Report. The Government has announced that the first step in the implementation of the Government response will be to release exposure draft legislation for public comment.

The ALRC recommended the Government initiate a review of the new credit reporting provisions five years after their commencement.[37] The Government will consider this recommendation in the Government response to the ALRC report.

[37] ALRC Report recommendation 54–8

Statement of Compatibility with Human Rights

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

This Bill is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview of the Bill

The Privacy Amendment Bill 2012 (the Bill) will amend the *Privacy Act 1988* (the Act) to implement the Government's first stage response to the Australian Law Reform Commission's report number 108 *For Your Information: Australian Privacy Law and Practice.* The ALRC, which had undertaken a comprehensive review of privacy law in Australia, released its report in May 2008. Given the large number of recommendations, the Government announced that it would respond in two stages. The Government's first stage response addressed 197 of the ALRC's 295 recommendations. The Bill implements the major elements of the first stage response.

The Bill will amend the Act to:

- create the Australian Privacy Principles (APPs), a single set of privacy principles applying to both Commonwealth agencies and private sector organisations, setting out the standards, rights and obligations for the collection, storage, security, use, disclosure and quality of personal information, which will replace the Information Privacy Principles (IPPs) for the public sector and National Privacy Principles (NPPs) for the private sector,
- introduce more comprehensive credit reporting, and
- clarify the functions and powers of the Privacy Commissioner and improve the Commissioner's ability to resolve complaints, recognise and encourage the use of external dispute resolution services, conduct investigations and promote compliance with privacy obligations.

The Bill will reduce complexity, increase consistency and clarify rights and obligations under the Act and improve usability for entities required to comply with the Act, while continuing to protect the privacy rights of individuals. The credit reporting provisions will be re-written to more effectively address the significant changes and increased practical complexity in the operation of the credit reporting system since the provisions were enacted in 1990. In introducing more comprehensive credit reporting the rights of individuals will be enhanced, including rights to access and correct their credit reporting information.

The Act currently provides for the development of APP Codes for particular sectors to guide their use of personal information. The Bill replaces the existing privacy codes and the credit reporting code with APP codes and the Credit Reporting Code of Conduct. The Bill will allow the Privacy Commissioner to create a binding code for the sector following consultation in circumstances where the private sector does not create its own Code, or the Code is found to not appropriately regulate the sector's use of information. All Codes, APP or Credit Reporting, are deemed disallowable legislative instruments by the amendments in the Bill, and will therefore be subject to Parliamentary scrutiny and accompanied by their own Statement of Compatibility with human rights.

Human rights implications

The Bill engages the following human rights:

- the protection against arbitrary interference with privacy
- the right to freedom of expression and opinion, and
- the right to a fair trial.

Protection against arbitrary interference with privacy

The Bill engages Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which provides that no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation, and that everyone has the right to the protection of the law against such interference or attacks.

The Bill protects against arbitrary interference with privacy by introducing a number of specific protections, including enhanced notification (APP 5), data quality (APP 10), data correction (APP 13) and dispute resolution mechanisms for individuals. In particular, these measures involve:

- enhancing obligations on agencies and organisations regarding an individual's access to, and correction of, their personal information, accompanied by a revised approach to complaints handling, including timeframes for notification and the use of alternative dispute resolution for credit reporting complaints, to more efficiently deal with complaints
- prohibiting the collection of credit reporting information about individuals reasonably known to be under 18
- in circumstances of suspected identity theft or fraud, providing individuals with the ability to prohibit, for a specified period of time, the disclosure of credit reporting information about them without their express authorisation
- requiring entities to develop and publish more comprehensive privacy policies to promote more open and transparent management of personal information
- introducing a requirement for Commonwealth government agencies to accord higher privacy protection to 'sensitive information'
- ensuring that personal information that is received by an entity is still afforded privacy protections, even where the entity has done nothing to solicit the information
- broadening the matters that that an individual is to be made aware of at the time of collection of the personal information of the individual
- introducing a new 'Direct Marketing' principle, that will place extra limitations on organisations that use or disclose personal information to promote or sell goods or services directly to individuals
- improving corrections and complaints processes for consumers, including allowing complaints to be made directly to the Privacy Commissioner in certain circumstances
- clarifying the functions and powers of the Privacy Commissioner to improve the Commissioner's ability to resolve complaints, recognise and encourage the use of external dispute resolution services, conduct investigations and promote compliance with privacy obligations
- ensuring the Commissioner has the flexibility to apply the Act to existing and emerging technologies and to enforce compliance where necessary, and

- requiring entities to ensure that obligations to protect personal information set out in the APPs cannot be avoided by disclosing personal information to a recipient outside Australia.

Reasonably necessary

A key objective of the Act is to balance the protection of the privacy of individuals, with the interests of public and private sector entities in carrying out their lawful and legitimate functions and activities. The Bill enables the personal information of an individual to be collected, used and disclosed in particular circumstances (e.g. APP 3 and APP 6). Collecting, using, storing and sharing personal information, including its release without an individual's knowledge or consent, all amount to interferences with privacy. In order for an interference with the right to privacy to be permissible, the interference must be authorised by law, be for a legitimate objective and be reasonable, necessary and proportionate to that objective.

One threshold standard that will apply in the APPs in certain circumstances is where an entity is able to undertake activities with personal information where it is 'necessary' for a particular purpose, function or activity. For example, an entity may collect sensitive information without consent if the entity reasonably believes that the collection is necessary to lessen or prevent a serious threat to the life, health or safety of an individual, or to public health and safety (APP 3.4 and s 16). These limitations are consistent with the prohibition on arbitrary interference with privacy as they are directed at legitimate objectives and are reasonable, necessary and proportionate to those objectives.

The Bill also enables the personal information of an individual to be collected, used and disclosed in certain circumstances where it is 'reasonably necessary' for one or more of the entity's functions or activities (agencies also have a 'directly related' test) (APP 3 and 6). It is reasonable for these entities to be able to handle personal information in these circumstances to promote the Government's service delivery, taxation, law enforcement and national security objectives, and the needs of business to offer services to the public. This is how the test has operated under the National Privacy Principles since their enactment in 2001. The permitted activities are limited to specific purposes (ie an entity's functions and activities), and subject to additional safeguards in the case of sensitive information. For these reasons, the 'reasonably necessary' threshold is consistent with the protection against arbitrary interference with privacy, subject to the additional safeguards in the case of sensitive information (APP 3.3 and 3.4).

Comprehensive credit reporting

The Bill implements the ALRC's recommendations to move to a more comprehensive credit reporting system. In this respect, the Bill may limit the prohibition on arbitrary interference with privacy by adding five new categories to the types of personal information that make up an individual's credit information in the credit reporting system. Four of the new categories, which are introduced in the new definition of *consumer credit liability information* in subsection 6(1), are:

- the type of credit account opened
- the date on which the consumer credit is entered into
- the date on which the consumer credit is terminated, and
- the current limit of the credit account.

The fifth category, repayment history information, is added directly to the definition of credit information, at part (c) of clause 6N of the Bill.

The Act currently enables the collection and disclosure of personal information that primarily detracts from an individual's credit worthiness—such as the fact that an individual has defaulted on a loan. This is commonly referred to as 'negative' or 'delinquency-based' credit reporting. The introduction of comprehensive credit reporting is aimed at providing a more balanced and accurate picture of an individual's credit situation than currently exists, providing positive information about a person's credit situation such as when an individual has met their credit payments. The introduction of more comprehensive credit reporting allows credit providers to access an enhanced set of personal information tools directly relevant to establishing an individual's credit worthiness. This will allow credit providers to make a more robust assessment of credit risk, which is expected lead to lower credit default rates. More comprehensive credit reporting is also expected to improve competition in the credit market, which may result in reductions to the cost of credit for individuals. The amendments will enable legitimate commercial activity, facilitating consumer lending and transactions, and thus the participation of individuals in the economy. These are legitimate objectives.

The Bill introduces a number of safeguards to provide individuals with the tools to access information held about them, and correct any inaccuracies. The Bill also makes improvements to the complaints process, to ensure that the first organisation to receive the individual's complaint is responsible for taking action. In moving to more comprehensive credit reporting it has been recognised that additional safeguards around the use of repayment history information, the fifth new category of information, are also necessary. Repayment performance history will only be available by credit providers who are licensees [and to lenders mortgage insurers in relation to services they provide to credit providers] and subject to the responsible lending obligations in the *National Consumer Credit Protection Act 2009 (Cth)*.[38]

The Bill continues to state clearly defined and limited uses and disclosures for credit reporting information. The Government did not support the ALRC's recommendation that secondary uses of credit reporting information should be subject to a broad discretion exercised by credit reporting bodies or credit providers. The Government's approach ensures any effect on privacy rights is proportionate and limited by the introduction of specific safeguards, including:

- only de-identified information can be used for the purpose of research, and the research must be reasonably connected to the credit reporting system, and
- the use of credit reporting information for the purposes of pre-screening is expressly limited to the purpose of excluding adverse credit risks from marketing lists.

Pre-screening is subject to specific requirements, including only the use of negative credit reporting information, the requirement for notice at the time of collection that information may be used for this purpose, an opt out opportunity, and a prohibition on individuals being identified for other direct marketing . Any entity involved in pre-screening must maintain auditable evidence to verify compliance, and which is available to individuals. Pre-screening is also only available to credit providers who are subject to the *National Consumer Credit Protection Act 2009* (NCCP Act).

[38] *National Consumer Credit Protection Act 2009*, Chapter 3.

In the consumer credit environment it is important to achieve a balance between privacy protection and the efficient operation of the credit market. Access to narrowly defined categories of credit information to ensure a more balanced picture of an individual's credit situation, taking into account positive action such as payment, and not just negative information like defaults, and to allow for more effective risk assessment by credit providers is balanced with the enhanced privacy protections set out above.

Any limitations on the prohibition against arbitrary interference with privacy in the Bill are clearly and narrowly defined, for the legitimate purpose of improving the management of personal and credit reporting information, and accompanied by sufficient safeguards to maintain reasonable privacy protections. The measures are reasonable, necessary and proportionate as they ensure the smallest possible set of data is used for the narrowest purposes to achieve the objective of providing a functional consumer credit market.

Freedom of expression

The Bill engages Article 19 of the ICCPR. Article 19 guarantees freedom of expression, including the right to impart and to receive information. The freedom of expression is not an absolute right, and Article 19(3) of the ICCPR specifies the legitimate aims which any legal restriction on the exercise of freedom of expression must pursue. In this case the Bill limits the right to freedom of expression in order to promote respect for the rights or reputations of others, namely the protection against arbitrary interference with privacy in Article 17.

The Commissioner has the ability to create binding codes in certain, defined circumstances (new Part IIIB inserted by Schedule 3). Codes will provide additional protections over and above the APPs. Codes cannot displace or provide for a lower standard of privacy protection than the APPs. The ability of the Commissioner to create binding codes may in certain circumstances limit the code developers' (which could be any entity subject to the Act) right to freedom of expression. Not every code will impinge on this right. The performance of the functions and powers of the Commissioner, including the development of a binding code, continue to be governed by Section 29 of the Act, which requires the Commissioner to have regard to, amongst other things, the protection of important human rights and social interests that compete with privacy.[39] Section 29 also provides that the Commissioner must take account of international obligations accepted by Australia and any developing international guidelines relevant to the better protection of individual privacy. When issuing directions and guidelines the Commissioner must also ensure they are consistent with any relevant APPs or credit reporting provisions. As noted above, all Codes will be disallowable legislative instruments, subject to Parliamentary scrutiny, and required to be accompanied by their own Statement of Compatibility with human rights. These safeguards ensure that the limitation the Bill places on the right to freedom of expression is reasonable, necessary and proportionate.

Fair trial

The Bill engages Article 14 of the ICCPR, which guarantees a person be afforded, in the determination of any criminal charge against them, the right to a fair trial. The United Nations Human Rights Committee has stated that the notion of criminal charges may 'also

[39] *Privacy Act 1988* (Cth) Part IV Division 2 s29(a)

extend to acts that are criminal in nature with sanctions that, regardless of their qualification in domestic law, must be regarded as penal because of their purpose, character or severity'.[40]

The Bill removes many of the criminal offences in the Act, replacing them with civil penalty provisions.[41] The civil penalty provisions, such as those in Subdivision D of Part IIIA, are declared not to be offences under Part VIB. While the provisions provide for significant civil penalties it is considered that serious breaches of privacy should attract serious penalties. This is consistent with the civil penalties in the NCCP Act, and with the Government's overall response to serious breaches by corporations.

The Bill incorporates appropriate safeguards into the civil penalty provisions of the Bill[42]. It stipulates that in determining pecuniary penalties a court must take all relevant matters into account, including the circumstances of the contravention, the nature and extent of any loss or damage suffered because of the contravention and whether the entity has previously been found to have engaged in similar conduct. The Bill provides that an entity will not be liable for more than one pecuniary penalty in relation to the same conduct. These provisions will ensure that pecuniary penalties are proportionate to any contravention of a civil penalty provision, and protect the rights expressed in Article 14.

Conclusion

The Bill is compatible with human rights because it advances the protection of human rights, primarily protection against arbitrary interference with privacy, and, to the extent that it may also limit other human rights, those limitations are reasonable and proportionate.

40 General Comment No. 32, para 15; Communication No. 1015/2001, *Perterer v. Austria*, para. 9.2.
41 Privacy Amendment Bill 2012 section ^164(4) of Part VIB
42 section ^164(5) of Part VIB

PRIVACY AMENDMENT (ENHANCING PRIVACY PROTECTION) BILL 2012

NOTES ON CLAUSES

List of Abbreviations

APP	Australian Privacy Principle
Information Commissioner	Australian Information Commissioner
IPP	Information Privacy Principle
NPP	National Privacy Principle
OAIC	Office of the Australian Information Commissioner
Privacy Act	Privacy Act 1988

NOTES ON CLAUSES

Clause 1 Short title

Clause 1 sets out the title by which the Bill, when enacted, is to be cited - *Privacy Amendment (Enhancing Privacy Protection) Act 2012*.

Clause 2 Commencement

Clause 2 inserts a table which provides for the commencement arrangements for each of the provisions in the table. Column 1 states the provision number, and column 2 provides the commencement arrangements for that particular provision.

The table provides that sections 1 to 3 and any other provision in the Act that is not provided for in the table commences on the day the Act receives the Royal Assent. The table also provides that Items 156 and 162 of Schedule 5 and Parts 1 and 4 of Schedule 6 also commence on the day the Act receives the Royal Assent.

The majority of the new provisions have a deferred commencement of 9 months from the day after the Bill receives the Royal Assent. This deferment is to allow agencies and organisations sufficient time to prepare for the introduction of the new provisions, particularly for the credit reporting provisions. The table in Clause 2 provides that the following provisions commence the day after the end of the period of 9 months beginning on the day this Act receives the Royal Assent:

Schedules 1 to 4, Items 1 to 70, 72 to 79, 81 to 131, 133 to 155, 157 to 161, 163 to 171, and 173 to 180 of Schedule 5, and Parts 2, 3, 5, 6, and 7 of Schedule 6.

Item 71 of Schedule 5 relates to the operation of the *Personally Controlled Electronic Health Records Act 2012* (Personally Controlled Electronic Health Records Act). Item 71 of Schedule 5 does not commence at all if section 73 of the Personally Controlled Electronic Health Records Act does not commence. If that provision does commence, Item 71 of Schedule 5 of this Bill commences immediately after its commencement, or the start of the day after the end of the period of 9 months beginning on the day this Bill receives the Royal Assent, whichever occurs later.

This situation also applies to Item 80 of Schedule 5, which relates to the operation of the Stronger Futures in the Northern Territory Act 2012 (Stronger Futures in the Northern Territory Act). Item 80 of Schedule 5 does not commence at all if section 105 of the Stronger Futures in the Northern Territory Act does not commence. If that provision does commence, item 80 of Schedule 5 commences immediately after its commencement, or the start of the day after the end of the period of 9 months beginning on the day this Bill receives the Royal Assent, whichever occurs later.

This commencement arrangement also applies to item 132 Schedule 5, which relates to the commencement of item 24 of Schedule 5 of the *Consumer Credit and Corporations Legislation Amendment (Enhancements) Act 2012*, and item 172 of Schedule 5 which relates to the commencement of item 32 of Schedule 1 of *Personally Controlled Electronic Health Records (Consequential Amendments) Act 2012*.

Clause 3 Schedule(s)

This clause provides for each Act specified in a Schedule to the Bill to be amended in accordance with the items set out in the relevant Schedule.

Schedule 1—Australian Privacy Principles

Introduction

Outline of this schedule

This schedule amends the Privacy Act to include the new Australian Privacy Principles (APPs). The APPs will be the cornerstone of the privacy protection framework of the Privacy Act. The APPs will replace the Information Privacy Principles (IPPs), which applied to Commonwealth agencies, and the National Privacy Principles (NPPs), which applied to certain private sector organisations. As with these former principles, the APPs will regulate the collection, holding, use and disclosure of personal information that is included in records. Schedule 1 also contains amendments to definitions to either replace or clarify them, or add more definitions to deal with new terms.

Principles based legislation

The APPs will be principles-based law. The best regulatory model for information privacy protection in Australia is this type of law. By continuing to use high-level principles, the Privacy Act regulates agencies and organisations in a flexible way. They can tailor personal information handling practices to their diverse needs and business models, and to the equally diverse needs of their clients.

The Privacy Act combines principles-based law with more prescriptive rules where appropriate. This regulation is complemented by guidance and oversight by the regulatory body, the Office of the Australian Information Commissioner (OAIC). This is comparable to international regulatory models in jurisdictions such as Canada, New Zealand and the United Kingdom.

Structure

The order in which the APPs appear is intended to reflect the cycle that occurs as entities collect, hold, use and disclose personal information.

This broadly consists of the following stages:

- planning in advance how to meet obligations in relation to the handling of personal information;
- considering whether information may or should be collected;
- collecting information;
- providing notification of collection to the individual concerned;
- using or disclosing the information for the purpose for which it was collected or for an allowable secondary purpose;
- maintaining the integrity of personal information by securely storing it and ensuring its quality; and
- when the information is no longer necessary for the functions or activities of the entity, destroying it or ensuring that it is no longer personal information.

To this end, the APPs have been set out in Parts that move through each of the above elements of the information-handling chain.

Part 1 sets out principles that require APP entities to consider the privacy of personal information, including ensuring that APP entities manage personal information in an open and transparent way.

Part 2 sets out principles that deal with the collection of personal information including unsolicited personal information.

Part 3 sets out principles about how APP entities deal with personal information and government related identifiers. The Part includes principles about the use and disclosure of personal information and those identifiers.

Part 4 sets out principles about the integrity of personal information. The Part includes principles about the quality and security of personal information.

Part 5 sets out principles that deal with requests for access to, and the correction of, personal information.

Key concepts – definition of 'personal information'

The definition of 'personal information' has been modified to implement the Government's acceptance of ALRC Recommendation 6-1.

It is important that this key definition be sufficiently flexible and technology-neutral to encompass changes in the way that information that identifies an individual is collected and handled. The ALRC's recommended definition continues to allow this approach and also brings the definition in line with international standards and precedents.

The proposed definition does not significantly change the scope of what is considered to be personal information. The application of 'reasonably identifiable' ensures the definition continues to be based on factors which are relevant to the context and circumstances in which the information is collected and held.

Consistent with the Government's response to ALRC Recommendation 6-2, the Government encourages the development and publication of appropriate guidance by the OAIC about the meaning of 'identified or reasonably identifiable'. This will be useful in assisting organisations, agencies and individuals to understand the application of the new definition, especially given the contextual nature of the definition.

Key concepts – 'reasonably necessary'

A number of the APPs allow for collection, use or disclosure where the entity believes that the collection, use or disclosure is 'reasonably necessary' for a particular purpose. It is intended that this be interpreted objectively and in a practical sense. It is not intended to provide a lower level of protection compared with the existing NPPs, where an objective test is implied.

In relation to the requirement that an entity must not collect, use or disclose personal information unless it is reasonably necessary for a particular purpose, function or activity, this is intended to reflect the following. The first is that the collection, use or disclosure is reasonably necessary to pursue that particular purpose, function or activity. Whether the collection, use or disclosure is reasonably necessary is to be assessed from the perspective of a reasonable person (not merely from the perspective of the entity proposing to undertake the activity).

Where a reasonable person would not regard the purpose, function or activity in question as legitimate for that type of entity, the collection, use or disclosure of personal information will not be 'reasonably necessary' even if the entity cannot effectively pursue that function or activity without collecting, using or disclosing the personal information.

Key concepts – requirement to take reasonable steps

A number of the APPs require an entity to take 'reasonable steps'. The expression 'such steps as are reasonable in the circumstances' is intended to be interpreted as being similar in meaning to the term 'reasonable steps' used in the NPPs. Specifically, the term requires an objective assessment, and the addition of the words 'in the circumstances' is only intended to highlight that when considering what are objectively reasonable steps the specific circumstances of each case must be considered. In some cases, the words '(if any)' are used to ensure that, in that particular case, if there are no steps that an entity needs to take to fulfil its obligations, it need not take any steps.

Key concepts – consent

Consent is a defined concept within the current Privacy Act which will be retained in the amended Act. Consent is defined to mean 'express consent or implied consent'. Express consent exists where a person makes an informed decision to give their voluntary agreement to collection, use or disclosure taking place.

Whether consent can be said to be implied depends entirely on the circumstances. Consent may be implied when, in the circumstances, the individual and the relevant entity have each engaged in conduct that means that it can be inferred the individual has consented, even though the individual may not have specifically stated that he or she gives consent.

Consent, in many circumstances, can be withdrawn at any time. In such circumstances, the consent no longer exists, and an entity would no longer be able to rely on consent having been given when dealing with the individual's personal information.

Consistent with the Government's response to ALRC Recommendation 19-1, the Government encourages the development and publication of appropriate guidance by the OAIC about what is required of agencies and organisations to obtain an individual's consent for the purposes of the Privacy Act.

Treatment of 'sensitive information'

Schedule 1 implements the Government's agreement with the ALRC that the community expects 'sensitive information' to be afforded higher privacy protections than personal information that is not sensitive. These protections will apply regardless of whether sensitive information is held by agencies or organisations. These requirements include that sensitive information may not be collected except where permitted by specified exceptions. These exceptions reflect the public interest in allowing entities to perform certain functions and activities.

Item 1 Section 3

Item 1 will amend section 3 of the Privacy Act by removing the reference to the 'transfer' of information. Section 3 provides that the Privacy Act does not affect the operation of State and Territory legislation that deals with the same subject matter and is capable of operating concurrently with the Privacy Act.

As a result of the changes in terminology from the NPPs to the APPs, reference to the 'transfer' of information is unnecessary. NPP 9 deals with transborder data flows and uses the term 'transfer'. However, APP 8, which deals with cross-border disclosure of personal information, uses the term 'disclosure'. The term 'transfer' is not otherwise used in the APPs. To ensure that section 3 accurately sets out the content of corresponding State and Territory privacy laws that are to be saved, it is necessary to omit reference to 'transfer'.

Item 2 Section 3 (note)

Item 2 will amend section 3 of the Privacy Act by replacing the reference to the NPPs with a reference to the APPs.

Item 3 Section 5

Item 3 will repeal section 5 of the Privacy Act, which is no longer necessary as it deals with the interpretation of the IPPs, which will be replaced by the APPs. New section 14 of the Privacy Act will note that the APPs are set out in Schedule 1 of the Privacy Act, and that a reference to an APP by a number is a reference to an APP with that number.

Item 4 Subsection 6(1) (paragraph (i) of the definition of 'agency')

Item 4 will repeal paragraph (i) of the definition of 'agency' in subsection 6(1) of the Privacy Act, which refers to an 'eligible case manager' (see Item 15).

Item 5 Subsection 6(1)

Item 5 will insert a definition of 'APP complaint' into subsection 6(1) of the Privacy Act. This definition means a complaint about an act or practice that, if established, would be an interference with the privacy of an individual because it breached an APP. A separate definition is required for an 'APP complaint' to distinguish it from other types of complaints under the Privacy Act (for example, 'code complaints', and complaints relating to the handling of credit reporting information).

Item 6 Subsection 6(1)

Item 6 will insert a definition of 'APP entity' into subsection 6(1) of the Privacy Act.

Under the current Act, the IPPs apply to Commonwealth agencies, while the NPPs apply to certain private sector organisations. Under the amendments in the Bill, both agencies and organisations will be regulated by the APPs. It is therefore necessary to include a definition that includes both types of entities.

Item 7 Subsection 6(1)

Item 7 will insert a definition of 'APP privacy policy' into subsection 6(1) of the Privacy Act. The definition is included in APP 1.3, which states that, '[a]n APP entity must have a clearly expressed and up-to-date policy (the APP *privacy policy*) about the management of personal information by the entity'. The intention of APP 1 is to ensure that APP entities manage personal information in an open and transparent way. APP 1 also contains requirements about the content of an APP privacy policy and its availability.

Item 8 Subsection 6(1)

Item 8 will insert a definition of 'Australian law' into subsection 6(1) of the Privacy Act. The definition addresses the Government's acceptance in principle of ALRC Recommendation 16-1 that it should include a reference to 'common law or equitable duties', but exclude 'contracts'. In that response, the Government also noted that while a definition will provide a degree of clarity, the meaning of 'law' is best determined on a case-by-case basis. The Government also outlined some relevant considerations in determining the application of the required or authorised by law exemption, but also in determining whether an applicable law is relevant under the Privacy Act.

The definition has been included to clarify the scope of provisions that allow collection, use or disclosure where it is required or authorised by or under law. Currently there is no definition of 'law' in the Privacy Act and it generally takes its ordinary meaning. The ALRC

found that there was a degree of uncertainty around the definition and that an inclusive definition should be expressly set out to create greater clarity.

Item 9 Subsection 6(1)

Item 9 will insert a definition of 'Australian Privacy Principle' into subsection 6(1) of the Privacy Act. The definition refers to section 14 of the amended Act, which is a provision ensuring that a reference in any Act to an APP by a number is a reference to the APP with that number.

Item 10 Subsection 6(1)

Item 10 will insert a definition of 'collects' into subsection 6(1) of the Privacy Act.

The definition will capture the substance of section 16B of the Privacy Act and IPPs 1-3, namely that the Privacy Act applies to personal information collected by entities regulated by the Privacy Act for inclusion in a record or generally available publication. Section 16B of the Privacy Act and the IPPs will be repealed.

Item 11 Subsection 6(1)

Item 11 will insert a definition of 'Commonwealth record' into subsection 6(1) of the Privacy Act, which will have the same meaning as in the *Archives Act 1983* (Archives Act). That expression appears in APPs 4 and 11, and ensures that certain requirements under the Archives Act relating to the retention of Commonwealth records will apply notwithstanding requirements in the APPs relating to destruction of personal information.

Item 12 Subsection 6(1)

Item 12 will insert a definition of 'court/tribunal order' into subsection 6(1) of the Privacy Act. The inclusion of orders of courts or tribunals as part of clarifying the scope of the 'required by or authorised by or under law' exceptions is ALRC Recommendation 16-1, which the Government accepted. This definition gives the broadest interpretation to the concept and is consistent with that terminology as it appears in other laws and regulations (for example, Legislative Instruments Regulations 2004).

Item 13 Subsection 6(1)

Item 13 will insert a definition of 'de facto partner' into subsection 6(1) of the Privacy Act. This contains a cross-reference to the meaning of that expression in the Acts Interpretation Act (see section 2D). This definition is relevant to subsection 6(10) of the Privacy Act, which provides that a 'de facto partner of the individual' is taken to be included within the concept of a 'family' for certain purposes.

Item 14 Subsection 6(1)

Item 14 will insert a definition of 'de-identified'. This will provide that personal information is 'de-identified' if the information is no longer about an identifiable individual or an individual who is reasonably identifiable. This term is used in the APPs and the credit reporting provisions.

Item 15 Subsection 6(1) (definition of 'eligible case manager')

Item 15 will repeal the definition of 'eligible case manager' in subsection 6(1) of the Privacy Act.

The concept of 'eligible case manager' came from the *Employment Services Act 1994*, which was repealed by the *Financial Framework Legislation Amendment Act (No. 1) 2006*. It is

therefore no longer necessary to include that definition. All references to 'eligible case manager' are being removed from the Privacy Act.

Item 16 Subsection 6(1) (after paragraph (b) of the definition of 'enforcement body')

Item 16 will insert a reference to the CrimTrac Agency into the definition of 'enforcement body' in subsection 6(1) of the Privacy Act.

The CrimTrac Agency is the national information-sharing service for Australia's police, law enforcement and national security agencies. It enables police agencies to share policing information with one another across Australia's state and territory borders. In view of its enforcement related functions and activities, and the type of information it collects, uses and discloses, it is appropriate to include the CrimTrac Agency in the definition of 'enforcement body'. This will enable it to collect personal and sensitive information for its legitimate functions and activities, and to enable such information to be used or disclosed on its behalf for an 'enforcement related activity'.

Item 17 Subsection 6(1) (after paragraph c) of the definition of 'enforcement body')

Item 17 will insert a reference to the 'Immigration Department'. That will be a new definition in section 6 of the Privacy Act referring to the Department administered by the Minister administering the *Migration Act 1958* (Migration Act).

Currently, this is a reference to the Department of Immigration and Citizenship (DIAC). The effect of this addition is that DIAC have the ability to collect personal and sensitive information for its functions and activities (subject to the additional requirement in APP 3.4 that the collection of sensitive information without consent be limited to its enforcement related activities), and will have the ability to have information used or disclosed on its behalf for an enforcement related activity.

In view of DIAC's enforcement related functions and activities, and the type of information it collects, uses and discloses, it is appropriate to include it in the definition of 'enforcement body'. However, given that it has a range of non-enforcement functions and activities, it will be limited in the collection of sensitive information to its 'enforcement related activities'.

Item 18 Subsection 6(1) (after paragraph (e) of the definition of 'enforcement body')

Item 18 will include the Office of the Director of Public Prosecutions (DPP) or similar bodies established under a law of a State or Territory in the definition of 'enforcement body' in subsection 6(1) of the Privacy Act. A body will be 'similar' to the DPP if it has similar enforcement related functions. A clear example of such a body is a State DPP.

The functions and activities of the Commonwealth and State/Territory DPPs include prosecuting criminal offences, preparing for, or conducting, proceedings before courts, and applying for orders relating to the confiscation of proceeds of crime. The DPP offices may, to some extent, come within the existing definition of 'enforcement body' through existing paragraphs (f) and (g) of that definition. However, to avoid any doubt about whether the DPP offices are enforcement bodies, it is necessary to include them in the definition.

Item 19 Subsection 6(1) (after paragraph (l) of the definition of 'enforcement body')

Item 19 will include the Corruption and Crime Commission of Western Australia (CCCWA) in the definition of 'enforcement body' in subsection 6(1) of the Privacy Act.

The CCCWA was established on 1 January 2004, under the *Corruption and Crime Commission Act 2003*, as a permanent investigative commission with the same powers as a Royal Commission. The CCCWA assists the Western Australia Police Service to combat organised crime by granting them special powers, and helps public sector agencies minimise and manage misconduct.

CCCWA is included for consistency, so that all currently-existing State integrity bodies are listed.

Item 20 Subsection 6(1)

Item 20 will insert a definition of 'enforcement related activity' into subsection 6(1) of the Privacy Act.

The definition will substantially capture the matters covered by NPP 2.1(h), which creates an exception to the prohibition against organisations using or disclosing personal information for a secondary purpose by listing a number of activities conducted by or on behalf of law enforcement bodies in respect of which personal information may be used or disclosed.

The definition of 'enforcement related activity' will replicate this list but add paragraphs to ensure that the definition covers the conduct of surveillance activities, intelligence gathering activities and other monitoring activities as well as protective or custodial activities. These types of activities have been included to update and more accurately reflect the range of activities that law enforcement agencies currently undertake in performing their legitimate and lawful functions.

The definition is used in APPs 6 and 8 and will enable certain uses and disclosures of personal and sensitive information which may otherwise be a breach of those APPs. The definition recognises that the limited use and disclosure of personal information for criminal law enforcement purposes is in the public interest when balanced with the interest in protecting an individual's privacy.

Item 21 Subsection 6(1)

Item 21 will insert a definition of 'entity' into subsection 6(1) of the Privacy Act.

In the amended Privacy Act, 'entity' will mean 'an agency, or an organisation or a small business operator'. Generally, while the APPs will not apply to small business operators, they may be regulated under provisions of Part IIIA (credit reporting).

Item 22 Subsection 6(1) (definition of 'generally available publication')

Item 22 will update the definition of 'generally available publication' in subsection 6(1) of the Privacy Act.

The new definition will explicitly state that a publication is a generally available publication whether or not payment of a fee is required to access it. The new definition is also more technologically neutral, in that it clearly covers material available electronically, including on the internet.

The amendment is not intended to suggest that any website or publication available on the internet is a generally available publication. An assessment must be made on a case-by-case basis, taking into account all relevant circumstances, such as the extent to which access to the publication or website is restricted in some way.

Item 23 Subsection 6(1)

Item 23 will insert a definition of 'government related identifier' into subsection 6(1) of the Privacy Act.

Government related identifiers are specifically assigned by one of a range of specifically listed government-related bodies (in paragraphs (a)-(d) of the definition) and are used to identify an individual or verify the identity of the individual. The definition extends to State and Territory authorities as well as Commonwealth agencies. Examples of government related identifiers include Medicare numbers and driver's licence numbers.

Item 24 Subsection 6(1)

Item 24 will insert a definition of 'holds' into subsection 6(1) of the Privacy Act.

The definition will substantially capture the concept formerly included in section 10 of the Privacy Act relating to record-keepers under the IPPs. That is, an entity holds personal information if the entity has possession or control of a record that contains the personal information.

Item 25 Subsection 6(1)

Item 25 will insert a definition of 'identifier' into subsection 6(1) of the Privacy Act. The concept is used in APP 9, which is concerned with the adoption, use or disclosure of government related identifiers by organisations.

The definition is broader than the definition of 'identifier' in NPP 7.3, in that it will apply to a number, letter or symbol, or combination of any or all of those things, that is used to identify or to verify the identity of the individual. As with the definition of 'identifier' in NPP 7.3, it will expressly exclude the individual's name, or the individual's ABN (within the meaning of the *A New Tax System (Australian Business Number) Act 1999*). It will also exclude anything else prescribed by the regulations to ensure that there is flexibility to exclude any future identifiers from the definition.

Item 26 Subsection 6(1)

Item 26 inserts a new definition of 'Immigration Department' in section 6 of the Privacy Act to refer to that Department administered by the Minister administering the Migration Act. Currently, that is DIAC.

Item 27 Subsection 6(1) (definition of 'Information Privacy Principle')

Item 27 will repeal the definition of 'Information Privacy Principle', which will no longer be necessary because the IPPs will be replaced by the APPs.

Item 28 Subsection 6(1) (definition of 'IPP complaint')

Item 28 will repeal the definition of 'IPP complaint', which will no longer be necessary because the IPPs will be replaced by the APPs. Complaints about acts and practices occurring after the commencement of the amendments, will relate only to the APPs.

Item 29 Subsection 6(1)

Item 29 will insert a definition of 'misconduct' into subsection 6(1) of the Privacy Act.

The new concept will assist in clarifying the scope of provisions that allow collection, use or disclosure of personal information for the purposes of taking action against persons who have engaged in serious misconduct. It includes fraud, negligence, default, breach of trust, breach of discipline or any other misconduct in the course of duty. It is intended that each of these terms will take their ordinary/common law meaning.

Item 30 Subsection 6(1) (definition of 'National Privacy Principle')

Item 30 will repeal the definition of 'National Privacy Principle', which will no longer be necessary because the NPPs will be replaced by the APPs.

Item 31 Subsection 6(1)

Item 31 will insert a definition of 'non-profit organisation' into subsection 6(1) of the Privacy Act.

The definition is based on the definition of 'non-profit organisation' in NPP 10.5, which states that '*non-profit organisation* means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade or trade union aims'. The amendment will update the definition so that the terms 'racial, ethnic' are included within 'cultural', as well as including 'recreational' purposes.

Item 32 Subsection 6(1) (definition of 'NPP complaint')

Item 32 will repeal the definition of 'NPP complaint', which is no longer necessary because the NPPs will be replaced by the APPs.

Item 33 Subsection 6(1)

Item 33 will insert a definition of 'overseas recipient' into subsection 6(1) of the Privacy Act.

The definition will refer to APP 8, which will deal with cross-border disclosure of personal information. In APP 8.1, an 'overseas recipient' is a reference to a person who is not in Australia or an external Territory and is not the entity holding the personal information or the individual who the personal information is about.

Item 34 Subsection 6(1)

Item 34 will insert a definition of 'permitted general situation' into subsection 6(1) of the Privacy Act. The definition refers to the new section 16A (see Item 82) which outlines situations where the collection, use or disclosure by an APP entity of personal information about an individual, or of a government related identifier, will not be a breach of the APPs.

Item 35 Subsection 6(1)

Item 35 will insert a definition of 'permitted health situation' into subsection 6(1) of the Privacy Act. The definition refers to the new section 16B (see Item 82) which outlines situations where the collection, use or disclosure of certain health information or genetic information, will not be a breach of the APPs.

Item 36 Subsection 6(1) (definition of 'personal information')

Item 36 will update the definition of 'personal information' in subsection 6(1) of the Privacy Act.

The new definition will reflect the Government's acceptance of the ALRC's recommendation that, 'personal information' should be defined as 'information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual' (ALRC Recommendation 6–1).

The definition in the Privacy Act refers to, 'information or an opinion (including information or an opinion forming part of a database)'. The reference to databases, which may have provided clarification in 1988 when the Privacy Act was passed, is no longer necessary and will not appear in the new definition. It is intended that information forming part of a database will be included in the new definition, even though databases are no longer specifically included in the definition.

The Privacy Act refers to 'an individual whose identity is apparent, or can reasonably be ascertained'. The new definition will use the terms 'identified' and 'reasonably identifiable'. The new definition has been cast in terms of identification of individuals because this

language is more consistent with the APEC Privacy Framework and other international instruments, which means that international jurisprudence and explanatory material will be more directly relevant to the Privacy Act.

The new definition will refer to an individual who is, 'reasonably identifiable'. Whether an individual can be identified or is reasonably identifiable depends on context and circumstances. While it may be technically possible for an agency or organisation to identify individuals from information it holds, for example, by linking the information with other information held by it, or another entity, it may be that it is not practically possible. For example, logistics or legislation may prevent such linkage. In these circumstances, individuals are not 'reasonably identifiable'. Whether an individual is reasonably identifiable from certain information requires a consideration of the cost, difficulty, practicality and likelihood that the information will be linked in such a way as to identify him or her.

In agreeing with ALRC Recommendation 6-2, the Government encouraged the development and publication of appropriate guidance about the meaning of 'identified or reasonably identifiable' in the definition of 'personal information' by the OAIC, noting that the decision to provide guidance was a matter for the OAIC. Guidance issued by the OAIC would play an important role in assisting organisations, agencies and individuals to understand the application of the new definition, especially given the contextual nature of the definition.

Item 37 Subsection 6(1) (definition of 'record')

Item 37 will amend the definition of 'record' in subsection 6(1). In order to allow for technological advances, 'record' will be defined inclusively rather than exhaustively.

Item 38 Subsection 6(1) (paragraphs (b) and (c) of the definition of 'record')

Item 38 will amend the definition of 'record' in subsection 6(1) to include reference to 'electronic or other device'. This picks up the Government's response to ALRC Recommendation 6-6, which is that the definition should encompass a broad range of recorded information, including information held in electronic format. This change will ensure that the definition is sufficiently flexible to encompass how information will be recorded and stored in the future.

Item 39 Subsection 6(1) (at the end of the definition of 'record')

Item 39 will add a note to the definition of 'record' in subsection 6(1). To promote consistent terminology with other Commonwealth legislation, the note will make it clear that the use of the term 'document' in the definition of 'record' is found in section 2B of the Acts Interpretation Act.

Item 40 Subsection 6(1)

Item 40 will insert a definition of 'responsible person' into subsection 6(1) of the Privacy Act. The definition will direct the reader to the new section 6AA (see Item 52).

Item 41 Subsection 6(1) (subparagraph (a)(viii) of the definition of 'sensitive information')

Item 41 will amend the definition of 'sensitive information' in subsection 6(1) to refer to an individual's sexual 'orientation' rather than 'preferences'. This minor change is not intended to change the meaning of the definition but will ensure consistency with other Commonwealth, state and territory legislation.

Item 42 Subsection 6(1) (at the end of the definition of 'sensitive information')

Item 42 will amend the definition of sensitive information in subsection 6(1) of the Privacy Act by adding references to biometric information and biometric templates.

The inclusion of these two paragraphs will implement the Government's response to ALRC Recommendation 6-4. The Government agreed with the ALRC that biometric information had similar attributes to other sensitive information and it was therefore desirable to provide it with a higher level of protection.

Given the broad nature of what can be considered biometric information, the definition makes it clear that the additional protections only extend to that biometric information which is specifically being collected for the purpose of automated biometric verification or biometric identification.

Item 43 Subsection 6(1) (definition of 'solicit')

Item 43 will repeal the definition of 'solicit' in the Privacy Act. A new definition of 'solicits' will be inserted (see Item 44).

Item 44 Subsection 6(1)

Item 44 will insert a new definition of 'solicits' into the Privacy Act.

The new definition will be based on the present definition but use the term 'entity' consistently with the terminology of the amended Privacy Act.

Item 45 Subsection 6(1) (definition of 'use')

Item 45 will repeal the definition of 'use' in Subsection 6(1) of the Privacy Act. The amended Privacy Act will contain a single principle applying to both use and disclosure, rendering this definition unnecessary. The concept of 'use' may still apply to any distinction between use and disclosure under the amended Privacy Act.

Item 46 Subsection 6(2)

Item 46 will repeal subsection 6(2) of the Privacy Act.

The subsection deals with breaches of the IPPs so will not be necessary in the amended Privacy Act.

Item 47 Paragraph 6(7)(a)

Item 47 will amend paragraph 6(7)(a) of the Privacy Act to refer to an 'APP' instead of an 'IPP' in the context of a complaint.

Item 48 Paragraph 6(7)(d)

Item 48 will repeal paragraph 6(7)(d) of the Privacy Act.

The paragraph refers to a 'file number complaint and an NPP complaint'. With the introduction of the APPs, this paragraph will not be necessary in the amended Privacy Act. The concept of a complaint being both a 'file number complaint and an APP complaint' will be covered under paragraph 6(7)(a) of the Privacy Act.

Item 49 Paragraph 6(7)(f)

Item 49 will amend paragraph 6(7)(f) of the Privacy Act to refer to an 'APP' instead of an 'NPP' in the context of a complaint.

Item 50 Subsection 6(10)

Item 50 will amend subsection 6(10) of the Privacy Act to refer to new section 16 instead of section 16E, which is being repealed by Item 82. The new section 16 confirms that the APPs do not apply to regulate the handling of personal information by an individual where that information is collected, held, used, disclosed or transferred for personal, family or household affairs (that is, done other than in the course of business). This is consistent with the exemption in subsection 7B(1).

Item 51 Paragraph 6(10)(a)

Item 51 will omit the reference to the Acts Interpretation Act in paragraph 6(10)(a) of the Privacy Act, which refers to de facto partners.

This reference will no longer be necessary, because the amended Privacy Act will contain a definition of 'de facto partner' which gives the term the meaning given by the Acts Interpretation Act (see Item 13).

Item 52 After section 6

Item 52 will amend the Privacy Act by inserting a definition of 'responsible person' after section 6. This definition replaces the definition in NPP 2.5, which contains a list of persons who are responsible for an individual under NPP 2.4. Some minor revisions have been made for consistency with terminology in other Commonwealth legislation.

NPP 2.4 provides that a health service may disclose health information about the individual to a person responsible for the individual in certain circumstances. NPP 2.4 has been replaced by new subsection 16B(5) (see Item 82).

Item 53 Section 6A (heading)

Item 53 will amend the heading to section 6A of the Privacy Act by referring to a breach of an APP instead of a NPP.

Items 54-59 Subsection 6A

Items 54-59 will amend various parts of section 6A of the Privacy Act by referring to the APPs instead of the NPPs.

Item 60 Subparagraphs 6C(4)(b)(ii) and (iii)

Item 60 will amend subparagraphs 6C(4)(b)(ii) and (iii) of the Privacy Act to remove the references to the transfer of information.

As a result of the changes in terminology from the NPPs to the APPs, reference to the 'transfer' of information is unnecessary. NPP 9 deals with transborder data flows and uses the term 'transfer'. However, APP 8, which deals with cross-border disclosure of personal information, uses the term 'disclosure'. To ensure that subparagraphs 6C(4)(b)(ii) and (iii) of the Privacy Act accurately reflect matters regulated by the Privacy Act or under State and Territory privacy laws, it is necessary to omit reference to 'transfer'.

Item 61 Subsection 6EA(1)

Item 61 will amend subsection 6EA(1) of the Privacy Act by removing the provision that section 16D does not apply to a small business operator if the small business operator chooses to be treated as an organisation and is registered under section 6EA.

This provision will be removed because section 16D, which deals with the delayed application of the NPPs to organisations that carry on one or more small businesses, will also be repealed.

Item 62 Paragraph 6F(3)(b)

Item 62 will amend paragraph 6F(3)(b) of the Privacy Act by removing the reference to the transfer of information. This is being done for the same reason outlined in Item 60. To ensure that paragraph 6F(3)(b) of the Privacy Act accurately reflect matters regulated by the Privacy Act, it is necessary to omit reference to 'transfer'.

Item 63 Paragraph 7(1)(a)

Item 63 will amend paragraph 7(1)(a) of the Privacy Act by removing the term 'eligible case manager' (see Item 15).

Item 64 Paragraph 7(1)(cb)

Item 64 will repeal paragraph 7(1)(cb) of the Privacy Act, which deals with acts done by an 'eligible case manager' (see Item 15).

Item 65 Paragraphs 7(1)(d) and (e)

Item 65 will amend paragraphs 7(1)(d) and (e) of the Privacy Act by removing the references to an 'eligible case manager' (see Item 15).

Item 66 Paragraphs 7(1)(ea) and (eb)

Item 66 will repeal paragraphs 7(1)(ea) and (eb) of the Privacy Act, which deal with the affairs of an 'eligible case manager' (see Item 15).

Item 67 Subsection 7(2)

Item 67 will amend subsection 7(2) of the Privacy Act by referring to the APPs instead of the IPPs and the NPPs.

Item 68 Subsection 7B(1) (note)

Item 68 will amend the note to subsection 7B(1) of the Privacy Act by replacing a reference to section 16E of the Privacy Act with a reference to the new section 16, which also addresses the application of the APPs to personal, family and household affairs. Section 16E is being repealed by Item 82.

Item 69 Subsections 7B(1) and (2) (notes)

Item 69 will amend the notes to subsections 7B(1) and (2) by referring to the APPs instead of the NPPs.

Items 70 and 71 Paragraph 8(2)(b) and subsection 8(2)

Items 70 and 71 will amend paragraph 8(2)(b) and subsection 8(2) of the Privacy Act by describing an agency as holding a record instead of being a record-keeper in relation to the record. This amendment will make the provision more consistent with the terminology in the Privacy Act with the repeal of the IPPs and the new inclusion of the new APPs.

Item 24 will insert a definition of 'holds' into subsection 6(1) of the Privacy Act. The new definition states that, 'an entity *holds* personal information if the entity has possession or control of a record that contains the personal information'. Therefore, it is necessary to amend paragraph 8(2)(b) and subsection 8(2) of the Privacy Act so that agency that was a record-keeper under the former IPPs in relation to a record, can simply be described as an agency holding a record.

Item 72 Section 9

Item 72 will repeal section 9 of the Privacy Act. Section 9 refers to 'collectors' of personal information, which is a term used in the IPPs. It also deemed the act of collection by an employee of an agency, staff member or special member of the Australian Federal Police, or for certain unincorporated bodies assisting or connected with an agency, as collections by those agencies in certain circumstances.

This provision is now unnecessary with the repeal of the IPPs. Under section 8 of the Privacy Act, acts and practices of employees of these entities, including the collection of personal information, will still be treated as acts and practices of the entities themselves.

Item 73 Section 10 (heading)

Item 73 will amend the heading to section 10 of the Privacy Act by referring to agencies taken to hold a record rather than record-keepers.

This amendment will make the heading consistent with Item 24, which will insert a definition of 'holds' into subsection 6(1) of the Privacy Act. The new definition states that 'an entity *holds* personal information if the entity has possession or control of a record that contains the personal information', so an agency that is a record-keeper in relation to a record can simply be described as holding the record. That definition will substantially capture the concept formerly included in section 10 of the Privacy Act relating to record-keepers under the IPPs.

Item 74 Subsections 10(1) to (3)

Item 74 will repeal subsections 10(1), (2) and (3) of the Privacy Act.

These subsections establish which agencies are record-keepers for the purposes of the Privacy Act. However, the amended Privacy Act will no longer use the term 'record-keeper' (see Item 73) so the subsections will not be necessary.

Item 75 Subsections 10(4) and (5)

Item 75 will amend subsections 10(4) and (5) of the Privacy Act by referring to agencies holding records rather than being 'record-keepers' in relation to records. As with the amendments in Items 24 and 73, this amendment reflects the repeal of the 'record-keeper' concept.

Item 76 Section 12

Item 76 will repeal section 12 of the Privacy Act.

Section 12 will no longer be necessary because it provides that the IPPs apply to agencies in possession of personal information. The APPs, which will replace the IPPs, will not maintain the distinction between possession and control which forms the basis of section 12.

Item 77 Subsection 13B(1) (note)

Item 77 will amend the note to subsection 13B(1) of the Privacy Act by replacing the references to the NPPs with references to the APPs.

Item 78 Subsection 13B(1) (note)

Item 78 will amend the note to subsection 13B(1) of the Privacy Act by replacing the reference to NPP 2 with a reference to APP 6, which will deal with use and disclosure of personal information.

Item 79 Subsection 13B(1A) (note)

Item 79 will amend the note to subsection 13B(1A) of the Privacy Act by replacing the reference to the NPPs with a reference to the APPs.

Item 80 Subsection 13C(1) (note)

Item 80 will amend the note to subsection 13C(1) of the Privacy Act by replacing the references to the NPPs with references to the APPs.

Item 81 Subsection 13C(1) (note)

Item 81 will amend the note to subsection 13C(1) of the Privacy Act by replacing the reference to NPP 2 with a reference to APP 6, which will deal with use and disclosure of personal information.

Item 82 Divisions 2 and 3 of Part III

Item 82 will repeal Divisions 2 and 3 of Part III of the Privacy Act. These Divisions provide for the application of the IPPs, the NPPs and approved privacy codes. The IPPs and NPPs will be replaced by the APPs, and so will no longer be necessary. A new Part IIIB will be inserted into the Privacy Act dealing with privacy codes.

Item 82 will insert new Divisions 2 and 3 of Part III into the Privacy Act. The new sections in these Divisions are outlined below.

Section 14 will direct the reader to the APPs in Schedule 1 of the Privacy Act, and provide that a reference in any Act to an APP by a number is a reference to the APP with that number.

Section 15 will provide that APP entities must not do an act, or engage in a practice that breaches an APP. This requirement replaces the requirement relating to the IPPs and the NPPs in sections 16 and 16A, which are being repealed.

Section 16 will express the same policy as section 16E of the Privacy Act, namely that the APPs will not apply to any dealings with personal information by an individual if the dealing is only for the purposes of, or in connection with, his or her personal, family or household affairs.

Section 16A will create the concept of a 'permitted general situation'. This will be a description of a situation that is permitted (ie, not a breach of privacy) in relation to the collection, use or disclosure of personal information by an APP entity in certain circumstances listed in a table. To come within the 'permitted general situation' concept, the table outlines particular entities, the type of information or identifier, and other specified conditions that need to be satisfied.

Prevention of serious threat to life, health or safety

Item 1 of the table in section 16A will enable an APP entity to collect, use or disclose personal information or a government related identifier in a permitted general situation without breaching the APPs.

The first condition is that it is unreasonable and impracticable to obtain the individual's consent to the collection, use or disclosure. This implements the Government's response to ALRC Recommendation 25-3 to include an additional safeguard to balance the removal of the 'imminent' element (for example, in IPP 10.1(b)). The ALRC believed that the 'imminent' requirement set a disproportionately high bar to the use and disclosure of personal information.

For the purposes of this exception, whether it was 'reasonable' to seek consent would include whether it is realistic or appropriate to seek consent. This might include whether it could be reasonably anticipated that the individual would withhold consent (such as where the individual has threatened to do something to create the serious risk). It would also likely be unreasonable to seek consent if there is an element of urgency that required quick action. Whether the individual had, or could be expected to have, capacity to give consent would also be a factor in determining whether it was 'reasonable' to seek consent.

Seeking consent would not be 'practicable' in a range of contexts. These could include when the individual's location is unknown or they cannot be contacted. If seeking consent would impose a substantial burden then it may not be practicable. It may also not be practicable to seek consent if the use or disclosure relates to the personal information of a very large number of individuals.

In assessing whether it is 'reasonable or practicable' to seek consent, agencies and organisations could also take into account the potential consequences and nature of the serious threat.

This approach creates a presumption that agencies and organisations should consider seeking consent before using or disclosing personal information in the circumstances set out in the recommendation.

Secondly, the act or practice will be permitted where the collection, use or disclosure of personal information or a government related identifier is necessary to lessen or prevent a serious threat to the life, health or safety of any individual or to public health or safety.

Unlawful activity

Item 2 of the table in section 16A will enable an APP entity to collect, use or disclose personal information or a government related identifier in a permitted general situation without breaching the APPs.

This will be where the APP entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to an entity's functions or activities has been, is being or may be engaged in; and the entity reasonably believes that the collection, use or disclosure of personal information or a government identifier is necessary in order for the entity to take appropriate action in relation to the matter.

The provision, by specifying that the unlawful activity or serious misconduct must relate to an entity's functions or activities, intends that the exception will apply to an entity's internal investigations. Examples of 'appropriate action' in this context may include collection, use or disclosure of personal information or a government identifier for an internal investigation in relation to internal fraud or breach of the Australian Public Service Code of Conduct.

Missing persons

Item 3 of the table in section 16A will enable an APP entity to collect, use or disclose personal information in a permitted general situation without breaching the APPs.

This will be where the entity reasonably believes that the collection, use or disclosure of personal information is reasonably necessary to assist any APP entity, body or person to locate a person who has been reported as missing, and the collection, use or disclosure complies with rules made by the Information Commissioner under sub-section (2). This amendment gives effect to the Government's response to ALRC Recommendation 25-2, where the Government decided that entities should be permitted to use or disclose personal information for the purpose of locating a reported missing person.

Matters which the Information Commissioner's rules should address include:

- that uses and disclosures should only be in response to requests from appropriate bodies with recognised authority for investigating reported missing persons;
- that, where reasonable and practicable, the individual's consent should be sought before using or disclosing their personal information;
- where it is either unreasonable or impracticable to obtain consent from the individual, any use or disclosure should not go against any known wishes of the individual;
- disclosure of personal information should be limited to that which is necessary to offer 'proof of life' or contact information; and
- agencies and organisations should take reasonable steps to assess whether disclosure would pose a serious threat to any individual.

Consistent with the requirements of the *Legislative Instruments Act 2003* (Legislative Instruments Act), the Information Commissioner should consult with relevant stakeholders in making these rules.

Legal or equitable claim

Item 4 of the table in section 16A will enable an APP entity to collect, use or disclose personal information where it is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim. This is intended to replicate NPP 10.1(e), which provides a similar exception.

An example of where this exception is intended to apply is where an individual has made a claim under their life insurance policy, and the insurer is preparing to dispute the claim and it needs to collect health or other sensitive information about the claimant and about witnesses in order to prepare its case.

Alternative dispute resolution

Item 5 of the table in section 16A will enable an APP entity to collect, use or disclose personal information where it is reasonably necessary for the purposes of a confidential alternative dispute resolution process.

The confidentiality safeguard included in the provision will limit the scope of the alternative dispute resolution exception and so ensure an additional protection for personal information.

Diplomatic or consular functions

Item 6 of the table in section 16A will enable an agency to collect, use or disclose personal information where that agency believes that the collection, use or disclosure is necessary for its diplomatic or consular functions or activities.

This is a new exception and is intended to clarify that such agencies can collect, use and disclose such information both within and outside Australia. Government officials from agencies such as the Department of Foreign Affairs and Trade (DFAT), who are based overseas, regularly collect and disclose to their home agencies in Australia personal information as part of their diplomatic and consular functions. It would be impractical for DFAT and other agencies to seek the consent of foreign government officials and other individuals, about whom these agencies report to Australia, to collect and disclose their personal information to the Australian Government.

Similarly, it is necessary for government officials based overseas to report to DFAT in Australia in discharging its consular responsibilities, especially in the event of an overseas crisis where overseas officials are expected to assist Australians.

Defence

Item 7 of the table in section 16A will enable the Defence Force to collect, use or disclose personal information where it reasonably believes that the collection, use or disclosure of that information is necessary for any of the following occurring outside of Australia at the external Territories:

- war or warlike operations;
- peacekeeping or peace enforcement; and
- civil aid, humanitarian assistance, medical or civil emergency or disaster relief.

This is a new exception and is intended to clarify the circumstances where the collection of sensitive information may occur without consent outside Australia, and where personal information generally may be disclosed to an overseas recipient. The Defence Force undertakes a range of activities in other countries that involve the collection and disclosure of personal information (sometimes in remote and emergency situations) and it is important that there is certainty about its ability to undertake these activities without breaching the APPs.

Subsection 16A(2)

As noted above, the Information Commissioner may make rules under subsection 16A(2). This amendment gives effect to the Government's response to ALRC Recommendation 25-2, where the Government decided that such rules should binding, and in the form of a legislative instrument.

Section 16B

As noted above, the existing health privacy and research provisions in the Privacy Act have been incorporated in these amendments. This is implemented through the operation of the APPs, new section 16B and the provisions dealing with guidelines for medical research, health and genetic information in sections 95, 95A and 95AA.

Section 16B will create the concept of a 'permitted health situation'. This will be a description of a situation that is permitted (ie not a breach of privacy) in relation to the collection, use or disclosure of certain health and genetic information by an organisation. This section is intended to reproduce the exceptions that applied under NPP 2.1(d), 2.1 (ea), 2.4, and 10.2–10.3. APP 6.4 replaces NPP 10.4.

Subsection 16B(1) replaces NPP 10.2 and will continue to allow an organisation to collect health information if the information is necessary to provide a health service to the individual and the collection is required or authorised by or under an Australian law, or where it is collected in accordance with certain rules established by competent health or medical bodies.

Subsection 16B(2) replaces NPP 10.3 and will continue to allow an organisation to collect health information about an individual for the purpose of research or the compilation of statistics relevant to public health or safety or for the management, funding or monitoring of a health service provided the safeguards included in paragraphs 16B(2)(a), (b), (c) and (d) are satisfied. These safeguards replicate the existing safeguards in NPP 10.3. APP 6.4 replaces the requirement in NPP 10.4 for an organisation to de-identify health information collected in accordance with NPP 10.3.

Subsection 16B(3) replaces NPP 2.1(d) and will continue to allow an organisation to use or disclose health information for a secondary purpose if:

- the use or disclosure is necessary for research, or the compilation or analysis of statistics relevant to public health or public safety,
- it is impracticable for the organisation to obtain the individual's consent to the use or disclosure;
- the use or disclosure is conducted in accordance with guidelines issued by the Information Commissioner under section 95A; and
- in the case of disclosure – the organisation reasonably believes that the recipient of the information will not disclose the health information or personal information derived from the health information.

Subsection 16B(4) replaces NPP 2.1(ea) and will continue to allow an organisation to use and disclose genetic information about an individual to a genetic relative in circumstances where the genetic information may reveal a serious threat to a genetic relative's life, health or safety. Subsection 16B(4) does not include the reference in NPP 2.1(ea) to 'whether or not the threat is imminent'. The words were initially included in the provision to make it clear that the limitation in other NPPs that a threat be both serious and imminent did not apply. This is no longer necessary as the corresponding APPs refer to serious threats rather than serious and imminent threats.

Subsection 16B(5) replaces NPP 2.4 and will continue to permit disclosure of an individual's health information by an organisation that provides a health service to a responsible person for an individual in certain circumstances.

The definition of responsible person will now be included in section 6 (see Item 52).

Section 16C

Section 16C is a key part of the Privacy Act's new approach to dealing with cross-border data flows. In general terms, there are currently two internationally accepted approaches to dealing with cross-border data flows: the adequacy approach, adopted by the European Union in the Data Protection Directive of 1996, and the accountability approach, adopted by the APEC Privacy Framework in 2004. NPP 9 was expressly based on the adequacy approach of the EU Directive. Under the new reforms, APP 8 and section 16C will introduce an accountability approach more consistent with the APEC Privacy Framework.

The accountability concept in the APEC Privacy Framework is, in turn, derived from the accountability principle from the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 1980. The OECD Guidelines did not define accountability, being content with a statement that 'a data controller should be accountable for complying with measures which give effect to the principles' contained in the Guidelines.

As part of the new accountability approach, section 16C will provide that an APP entity will be taken to have breached the APPs:

- if an APP entity discloses personal information about an individual to an overseas recipient,
- APP 8.1 applies to that disclosure,
- the APPs do not apply under the Privacy Act to acts done, or practices engaged in, by the overseas recipient in relation to the information, and

- the overseas recipient does something that would be a breach of the APPs if the APPs had applied to those acts or practices.

The section complements APP 8, which contains key aspects of the accountability approach in the Privacy Act. Under APP 8.1, there is a positive requirement on entities to take reasonable steps to ensure the recipient will protect the information consistent with the APPs prior to any cross-border transfer occurring. More information about the operation of APP 8 is included below.

Item 83 Section 37 (table items 6 and 7)

Item 83 will repeal table items 6 and 7 in section 37 of the Privacy Act, thereby removing the references to eligible case managers (see Item 15).

Item 84 Subsections 54(2) and 57(2) (definition of 'agency')

Item 84 will amend subsections 54(2) and 57(2) of the Privacy Act by removing the reference to an 'eligible case manager' (see Item 15).

Items 85 and 86 Paragraph 80H(2)(e) and subparagraph 80P(1)(c)(v)

Items 85 and 86 will amend paragraph 80H(2)(e) and subparagraph 80P(1)(c)(v) of the Privacy Act by using the term 'responsible person' or 'responsible persons' instead of 'people who are responsible'. These amendments are required as a consequence of the inclusion of a definition of 'responsible person' which will be inserted into the Privacy Act by Items 40 and 52 to replace NPP 2.5.

Item 87 Paragraph 80Q(1)(c)

Item 87 will replace a reference to a person responsible for the individual in paragraph 80Q(1)(c) of the Privacy Act with the term 'responsible person' (see Items 85 and 86).

Guidelines for medical research, health and genetic information

As noted above, the existing health privacy and research provisions have been incorporated in these amendments. There are some consequential amendments to the provisions dealing with guidelines for medical research, health and genetic information in sections 95, 95A and 95AA to reflect the changes made by replacing the references to the IPPs or NPPs with references to the APPs or to new sections, particular APPs or to be consistent with relevant new sections.

Item 88 Subsection 95(1)

Item 88 will amend subsection 95(1) of the Privacy Act by clarifying that section 95 applies to agencies and not organisations. This preserves the existing operation of this section.

Item 89-99

These Items make consequential amendments to sections 95, 95A and 95AA.

Item 100 Subsection 95B(1)

Item 100 will amend subsection 95B(1) of the Privacy Act by referring to the APPs instead of the IPPs.

Item 101 Section 95C

Item 101 will amend section 95C of the Privacy Act by referring to the APPs instead of the NPPs.

Item 102 Subsections 100(2) to (4)

Item 102 will repeal subsections 100(2), (3) and (4) of the Privacy Act and substitute two replacement subsections. These provisions enable the Governor-General to make regulations that prescribe a government related identifier, an organisation, a class of organisations, and circumstances for the purposes of APP 9.3. These changes are necessary because of the replacement of NPP 7 (identifiers) with APP 9 (adoption, use and disclosure of government related identifiers).

Consistent with this change, the provisions will apply to 'government related identifiers' rather than 'identifiers'. As noted in Item 23, 'government related identifiers' are specifically assigned by one of a range of specifically listed government-related bodies and used to identify an individual or verify an individual's identity.

The regulation making power in subsection 100(2) will be based on the existing subsection 100(2) but will be different in two respects. First, it will be broadened to enable classes of organisations, as well as individual organisations, to be prescribed. This approach would still require that the Government clearly articulate the types of organisations that can interact with agency identifiers to provide services which are for the public benefit and for a list of the organisations to be publicly available, however it would not require continual updates to regulations to take to take account of new organisations.

New subsection 100(2) will also extend to State and Territory authorities as well as Commonwealth agencies. That will mean the Minister, amongst other things, will need to be satisfied that a relevant agency or State or Territory authority (or principal executive of such an agency or authority) has agreed to the matters to be prescribed, and has consulted the Information Commissioner about these matters.

New subsection 100(2) will also retain the requirement that the Minister is satisfied that the adoption, use or disclosure of the identifier by the organisation, or the class of organisations, in the circumstances can only be for the benefit of the individual to whom the identifier relates.

Under new subsection 100(3), the requirements in subsection 100(2) will not apply to regulations made in relation to certain uses or disclosures of Commonwealth payroll numbers and in the provision of superannuation services by an organisation to Commonwealth employees. That is, in making such regulations there does not have to be consultation with each individual agency affected. However, the Minister will still be required to consult with the Information Commissioner before making such regulations.

Item 103 Part X

Item 103 will repeal Part X of the Privacy Act, which contains consequential amendments.

Item 104 Schedules 1 and 3

Item 104 will repeal Schedules 1 and 3 of the Privacy Act, which respectively contain consequential amendments and the NPPs. The new Schedule 1 will contain the APPs.

Schedule 1—Australian Privacy Principles

Schedule 1 contains the 13 APPs, which are contained in five Parts. The five Parts are:

Part 1 sets out principles that require APP entities to consider the privacy of personal information, including ensuring that APP entities manage personal information in an open and transparent way.

Part 2 sets out principles that deal with the collection of personal information including unsolicited personal information.

Part 3 sets out principles about how APP entities deal with personal information and government related identifiers. The Part includes principles about the use and disclosure of personal information and those identifiers.

Part 4 sets out principles about the integrity of personal information. The Part includes principles about the quality and security of personal information.

Part 5 sets out principles that deal with requests for access to, and the correction of, personal information.

Part 1—Consideration of personal information privacy

Australian Privacy Principle 1—open and transparent management of personal information

APP 1 requires APP entities to manage personal information in an open and transparent way. This inclusion of APP 1 will keep the Privacy Act up-to-date with international trends that promote a 'privacy by design' approach, that is, ensuring that privacy and data protection compliance is included in the design of information systems from their inception.

APP 1 requires an APP entity to consider how it will handle personal information in compliance with the APPs or a registered APP code. Under APP 1.2 an APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions and activities that will ensure compliance with the APPs or a registered APP code that binds the entity. These practices, procedures and systems must also enable the entity to deal with inquiries or complaints from individuals.

The expression 'such steps as are reasonable in the circumstances' is intended to be interpreted as being similar in meaning to the term 'reasonable steps' used in the NPPs. Specifically, the term requires an objective assessment, and the addition of the words 'in the circumstances' is only intended to highlight that when considering what are objectively reasonable steps, the specific circumstances of each case must be considered.

Policies and practices under APP 1.2 could include:

- training staff and communicating to staff information about the agency or organisation's policies and practices;
- establishing procedures to receive and respond to complaints and inquiries;
- developing information to explain the agency or organisation's policies and procedures; and
- establishing procedures to identify and manage privacy risks and compliance issues, including in designing and implementing systems or infrastructure for the collection and handling of personal information by the agency or organisation.

APP 1.3 will require entities to have a clearly expressed and up-to-date privacy policy about the management of personal information by the entity. An 'up-to-date' privacy policy should be a privacy policy that is a 'living document' and is reviewed regularly.

Under APP 1.4, these policies must contain certain information relating to the kinds of personal information collected and held; how such information is collected and held; the purposes for which the entity collects, holds, uses and discloses personal information; access

and correction procedures; complaint-handling procedures; and information about any cross-border disclosure of personal information that might occur.

Where agencies or organisations have particularly significant information handling practices, these should be included in their privacy policies by clearly setting out how they collect, hold, use and disclose personal information. For example, where agencies or organisations have specific information retention or destruction obligations, these should be described as a necessary part of how they handle personal information.

Under APP 1.5, APP entities must take such steps as are reasonable in the circumstances to make their privacy policies available to the public free of charge, and in such form as is appropriate. As noted at the foot of APP 1.5, an APP entity will usually make its privacy policies available on its website. The inclusion of this note implements recommendation 6 of the Senate Committee, which considered that the requirement for an entity to make its privacy policy available in 'such form as is appropriate' should be further clarified.

Under APP 1.6, if a person or body requests a copy of the APP privacy policy of an APP entity in a particular form, the entity must take such steps as are reasonable in the circumstances to give the person or body a copy in that form. The inclusion of a 'body' picks up a suggestion of the Senate Committee, which considered that the intent of the provision should be clarified so that entities other than individuals (for example, media organisations) should be able to request a copy of the policy.

Australian Privacy Principle 2—anonymity and pseudonymity

APP 2 provides that individuals must have the option of dealing with an agency or organisation anonymously or through use of a pseudonym in relation to a particular matter. The principle emphasises that it is often not necessary for an entity to identify the individuals with whom they are dealing. The privacy of individuals will be enhanced if their personal information is not collected unnecessarily.

An APP entity will not be required to comply with APP 2 where that entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves. This is likely to be applicable in certain instances for agencies. For example, if individuals are required under an Australian law to identify themselves to an agency, then it will not be lawful or practical for the agency to deal with them anonymously or pseudonymously.

An APP entity will also not be required to comply with APP 2 where it is impracticable for the APP entity to deal with individuals who have not identified themselves (ie where individual seeks to remain anonymous or uses a pseudonym). For example, if a service delivery agency cannot deal with an individual without identification (for example, in collecting personal information for an application for a benefit), that agency would not be required to allow that individual to have the option of anonymity when dealing with them on that particular matter. A similar instance would be where a law enforcement agency is investigating a criminal offence and requires a person's identity to assist in that investigation. There may also be circumstances where the nature of a business and the service provided by an organisation is not compatible with providing the option to interact anonymously.

Australian Privacy Principle 3—collection of solicited personal information

APP 3 outlines the rules applying to the collection of personal information and sensitive information.

In terms of personal information other than sensitive information, there will be separate conditions for the collection of solicited personal information by agencies and organisations. This addresses concerns raised by the Senate Committee about whether organisations should be able to collect personal information in the same manner as agencies (ie where collection is 'directly related to' one or more of the entity's functions and activities). The Senate Committee believed that this approach may lower privacy protections and did not support it.

In relation to the requirement that an entity must not collect personal information unless it is reasonably necessary for the entity's functions or activities, this is intended to operate objectively and practically in the following manner.

First, the information collected is reasonably necessary to pursue that function or activity. Whether the collection is reasonably necessary is to be assessed from the perspective of a reasonable person (not merely from the perspective of the collecting entity). An entity's functions or activities are only those functions or activities that are legitimate for that type of entity. .

If an agency or organisation cannot, in practice, effectively pursue a legitimate function or activity without collecting personal information, then the collection of that personal information would be regarded as necessary for that legitimate function or activity. Where a reasonable person would not regard the function or activity in question as legitimate for that type of entity, the collection of personal information will not be 'reasonably necessary' even if the entity cannot effectively pursue that function or activity without collecting the personal information. An agency or organisation should not collect personal information on the off-chance that it may become necessary for one of its functions or activities in the future, or that it may be merely helpful.

The interpretation of the 'reasonably necessary' test applies throughout the APPs and not just in relation to APP 3.

Under APP 3.1, an agency must not collect personal information unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.

The 'directly related to' test ensures that there must be a clear connection between the collection of personal information and the agency's functions or activities. The 'directly related to' test was contained in IPP 1, which applied to agencies. The test will be retained in APP 3 because there may be agencies that need to collect solicited personal information in order to carry out legitimate and defined functions or activities, but may not be able to meet the 'reasonably necessary' test. While the 'directly related to' test may, depending on the circumstances, be a slightly lower threshold, agencies are subject to a wider range of accountability mechanisms (for example, through the Ombudsman, Ministers and the Parliament) in relation to information that they handle.

Under APP 3.2, an organisation must not collect personal information unless the information is reasonably necessary for one or more of the organisation's functions or activities. As noted above, the inclusion of the 'reasonably necessary' test for organisations, implements the views of the Senate Committee.

APP 3.3 will provide for the collection of 'sensitive information', which is a subset of personal information. The definition of sensitive information is in subsection 6(1) of the Privacy Act. As noted above, that definition now applies to agencies, and includes biometric information and biometric templates. The general rule is that sensitive information can only be collected by agencies or organisations where the collection meets the criteria outlined in APP 3.1 and APP 3.2 and where the individual has consented to the collection.

However, APP 3.4 will provide for exceptions to this general rule. These have been included to enable the collection of sensitive information without consent where it is in the public interest to do so when balanced with the interest in protecting an individual's privacy. These exceptions are outlined in detail below.

APP 3.4(a) Where required or authorised by or under Australian law or a court/tribunal order

This exception is intended to allow an APP entity to collect sensitive information without consent where it is required or authorised by or under Australian law or a court/tribunal order. An example of this involving sensitive information would be section 261AA of the Migration Act, which provides that a non-citizen migration detention must (other than in the prescribed circumstances) provide to an authorised officer one or more personal identifiers.

APP 3.4(b) Permitted general situations

See discussion about this exception at Item 82, section 16A.

APP 3.4(c) Permitted health situation

See discussion about this exception at Item 82, section 16B.

APP 3.4(d) Enforcement bodies

This exception is intended to allow an enforcement body (other than the Immigration Department), to collect sensitive information without consent where it reasonably believes that the collection is reasonably necessary for, or directly related to, one or more of the entity's functions or activities. The definition of 'enforcement body' is in subsection 6(1) of the Privacy Act.

Where the enforcement body is the Immigration Department, it will be able to collect sensitive information without consent where it reasonably believes that the collection is reasonably necessary for, or directly related to, one or more 'enforcement related activities' conducted by that Department.

The first part of this exception is necessary to enable agencies with law enforcement functions and activities to be able to collect sensitive information without consent to perform their lawful and legitimate functions and activities. There is a strong public interest in enabling law enforcement agencies to enforce the criminal law. A major part of this important function is the ability to collect information about individuals. An additional safeguard is that these agencies are also subject to significant accountability and oversight arrangements over their activities.

The second part of this exception is necessary to enable the Immigration Department to collect sensitive information without consent to perform their lawful and legitimate enforcement related activities. This Department has a wide range of enforcement related activities such as detecting, preventing, investigating and prosecuting breaches of visa, immigration and citizenship law; preventing and reducing irregular migration, people smuggling and trafficking in persons; collecting information to assess the criminal history of applicants for Australian citizenship; and cooperation with other agencies, including information-sharing, for law enforcement and border security purposes, and the protection of the public revenue.

However, the Immigration Department has a wider range of non-enforcement functions and activities than other enforcement bodies, and there is less justification for allowing those to come within the scope of this exception. Accordingly, the exception has been limited to where the Immigration Department reasonably believes that the collection is reasonably

necessary for, or directly related to, one or more 'enforcement related activities' conducted by that Department.

APP 3.4(e) Non-profit organisations

This exception is similar to NPP 10.1(d) and enables a non-profit organisation to collect sensitive information without consent if it relates to the activities of the organisation, and the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities.

Means of collection

APP 3.5 provides that an APP entity must collect personal information only by lawful and fair means. This is based on NPP 1.2. It is an important safeguard to ensure that personal information can only be collected by lawful and fair means. The OAIC has interpreted 'fair' to mean without intimidation or deception. The concept of fair would also extend to the obligation not to use means that are unreasonably intrusive.

APP 3.6 provides that an APP entity must collect personal information about an individual only from the individual. However, there are two exceptions to this general rule.

First, an agency may collect from a third party where the individual has consented to that collection; or where it is authorised or required under Australian law, or a court/tribunal order. In the context of dealings with government agencies, the ability for an individual to consent would minimise the need for that individual to provide the same personal information to different agencies. This will assist in giving effect to the Government's 'tell us once' service delivery reform policy.

Secondly, an APP entity may collect from a third party where it is unreasonable or impractical to collect that personal information directly from the individual. This is a particularly important exception for agencies. For example, a law enforcement agency may be investigating an individual for a criminal offence, but could prejudice that investigation by being forced to seek particular information directly from the individual. This exception will allow that long-standing type of activity to continue without breaching APP 3.

Solicited personal information

APP 3.7 provides that APP 3 applies to the collection of personal information that is solicited by an APP entity. As noted above, the concept of soliciting personal information refers to the situation where an entity requests another entity (which includes an individual) to provide the personal information, or to provide a kind of information in which that personal information is included. If an entity has not requested the personal information, but only received it from another entity (including where, for example, a law enforcement agency has asked another agency to examine the personal information), that will not be a solicited collection covered by APP 3. However, as noted below, where personal information is unsolicited, it will still be required to be handled in accordance with other relevant APPs, if it is not destroyed or de-identified.

Australian Privacy Principle 4—dealing with unsolicited personal information

APP 4 will ensure that personal information that is received by an entity is still afforded privacy protections, even where the entity has done nothing to solicit the information.

Under APP 4.1, where unsolicited personal information is received by an APP entity, the entity must, within a reasonable period, determine whether it could have collected the information under APP 3 as if it had solicited the information. If it could have been collected, APPs 5 to 13 will apply to that information as if it had been solicited.

To enable the APP entity to determine whether it could have collected the information, APP 4.2 allows that entity to use or disclose the personal information for that limited purpose.

APP 4.3 provides that, if the APP entity could not have collected the information, and if the information is not contained in a Commonwealth record, the entity must take steps to destroy the information or ensure that it is no longer personal information (for example, by taking steps to remove any reference to the individual to whom the information relates). Information will no longer be personal information when it does not satisfy the definition of 'personal information' in section 6 of the Privacy Act. The compliance burden entailed by APP 4 will be eased by the provision that the entity must destroy the personal information 'as soon as practicable'.

The reference in APP 4.3 to information 'contained in a Commonwealth record' ensures that the requirements on agencies to retain such information under the Archives Act will override the APP 4 destruction or de-identification requirements.

APP 4.3 contains the important qualifier 'only if it is lawful and reasonable to do so'. An example of where this would be applicable is where an APP entity has received unsolicited personal information from a law enforcement agency to assist that agency in its investigations. If the APP entity decides that it could not have collected the information, it would normally have to destroy it in accordance with APP 4.3. However, it would not be 'lawful and reasonable' to destroy such information until the assistance that the entity has given to the law enforcement agency has ended.

Under APP 4.4, if the APP entity cannot destroy or de-identify the information under APP 4.3 (because the information is contained in a Commonwealth record or because it would not be lawful and reasonable to do so), it must still handle the personal information in accordance with APPs 5 to 13. This will ensure that the information will be accorded the same privacy protections as any other personal information being held by the entity.

It is not the intention of APP 4 to prevent the practice of agencies forwarding incorrectly addressed correspondence. As noted in responses to the Senate Committee, the receipt of correspondence by Ministers, Members of Parliament and government departments and agencies would, in normal circumstances, be unsolicited. Under APP 4, these entities must, within a reasonable period after receiving the information, determine whether the unsolicited personal information could have been collected under APP 3 if the entity had solicited the information. It is clear that, in some circumstances, where considering and responding to concerns of members of the public, and referring them to appropriate recipients, are legitimate functions of the entity, the unsolicited information could have been collected under APP 3. Once an entity has determined that the personal information could have been collected under APP 3, it would be possible for the entity to use or disclose the information under APP 6.

Under APP 6, disclosure to another Minister or government department would be permitted where the individual has consented to the use and disclosure. Consent may be implied if it may reasonably be inferred in the circumstances from the conduct of the individual. Disclosure would also be permitted under APP 6 where the disclosure is related to the primary purpose of collection (or directly related, if the information is sensitive information), and the disclosure is within the individual's reasonable expectations. As the individual has written with queries, views or representations on particular issues, it is within their reasonable expectation that their correspondence will be referred to the appropriate entity within parliament or government.

Australian Privacy Principle 5—notification of the collection of personal information

APP 5 sets out the obligation for an entity to ensure that an individual is aware of certain matters when it collects that individual's personal information. Generally, the individual must be made aware of how and why personal information is, or will be, collected and how the entity will deal with that personal information.

APP 5.1 creates the general requirement for an APP entity to provide notification. That must occur at or before the time or, if that is not practicable, as soon as practicable after the APP entity collects personal information about an individual. At that time (whichever is relevant), the APP entity must take such steps (if any) as are reasonable in the circumstances to notify the individual of such matters referred to in APP 5.2 as are reasonable in the circumstances or otherwise ensure that the individual is aware of any such matters.

The phrase 'reasonable in the circumstances' is an objective test that ensures that the specific circumstances of each case have to be considered when determining the reasonableness of the steps in question. This flexibility is necessary given the different types of APP entities and functions/activities that are to be regulated under the APPs. In many cases, it would be reasonable in the circumstances for an APP entity to provide the information outlined in APP 5.2.

However, for agencies with particular functions and activities, this may not be the case. For example, it would not be reasonable in the circumstances for a law enforcement agency to notify an individual, who is under investigation for a criminal offence, particularly where that agency is undertaking covert surveillance, that information is being collected about them.

APP 5.2 lists specific matters of which the individual must be notified. This is based on IPP 2 and NPP 1.3 and, coupled with APP 1, is intended to give the individual detailed and enhanced information about how their personal information is to be handled by an APP entity. This information includes contact details of the APP entity; whether information has been collected from a third party or under an Australian law or court/tribunal order (and details about that collection); the purpose of the collection; complaint-handling and access/correction information in the APP entity's privacy policy; disclosure information, including to overseas recipients, and the consequences of not collecting the information.

Part 3—Dealing with personal information

Australian Privacy Principle 6—use or disclosure of personal information

APP 6 sets out the circumstances in which entities may use or disclose personal information that has been collected or received. This APP is based on IPPs 10 and 11, and NPPs 2 and 10. As with those principles, it is implicit from the principle that entities may use or disclose personal information for the primary purpose for which the information was collected. This is outlined in general in APP 6.1, which creates the general prohibition on secondary disclosure.

The provision allows for a situation where there is a general primary purpose (for example, assessing a person's suitability to enter Australia). How broadly the primary purpose can be described will need to be determined on a case-by-case basis and it will depend on the circumstances.

The Government anticipates that the OAIC will develop specific guidance about the meaning of 'primary purpose' in consultation with agencies and organisations.

Generally, personal information must only be used or disclosed for purposes other than the primary purpose, that is, for a secondary purpose, if the relevant individual has consented, or

exceptions in APP 6.2 and 6.3 apply. These exceptions list a number of specific circumstances in which allowing secondary disclosure is in the public interest when balanced with the interest in protecting an individual's privacy.

The exceptions will apply to sensitive information as well as to other personal information. In the particular case where the individual would reasonably expect the entity to use or disclose the information for the secondary purpose:

- for *sensitive information*, the use or disclosure must be directly related to the primary purpose;
- for personal information which is not sensitive information, the use or disclosure must be related to the primary purpose.

As with APP 3, there are a number of exceptions enabling the use or disclosure of personal and sensitive information where 'required or authorised by or under Australian law or a court/tribunal order'; in permitted general situations (section 16A); in permitted health situations (section 16B); and where an 'APP entity reasonably believes that the use of disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body'. The final exception is aimed at enabling any APP entity to cooperate with an enforcement body where it may have personal information relevant to an enforcement related activity of that enforcement body.

APP 6.3 will provide that an agency will be allowed to disclose biometric information or templates if the recipient is an enforcement body and the disclosure is conducted in accordance with the guidelines made by the Commissioner. This approach recognises that non-law enforcement agencies have current, and will have future, legitimate reasons to disclose biometric information and templates to enforcement bodies. A practical example of the effect of this option would be to enable, consistent with the Commissioner's guidelines, the automatic provision of biometric information and templates by a non-enforcement agency into a database operated by an enforcement body. This is currently a gap in the enforcement related activity exception in the Privacy Act that prevents this increasing activity from occurring. The privacy safeguard for this new proposal is that the activity in question would be subject to ongoing oversight by the Information Commissioner through guidelines; this recognises that there are likely to be continuing developments in the use of biometric information and templates, and ongoing questions about the appropriate use of this evolving technology.

APP 6.4 provides that, if an APP entity collects health information about an individual for certain research purposes under subsection 16B(2), that entity must take such steps as are reasonable in the circumstances to de-identify that information before it uses or discloses the information under APP 6.1 or 6.2. This reproduces the requirement in NPP 10.4.

APP 6.5 will provide that if an entity uses or discloses personal information because it is reasonably necessary for an enforcement related activity, the entity must make a written note of the use or disclosure. The requirement is based on NPP 2.2 and aims to ensure accountability for such disclosures, but will not be extended to other exceptions to the rule against use or disclosure for a secondary purpose because of the compliance burden it would impose on entities.

APP 6.6 will provide that if a corporation collects personal information and passes it on to a related corporation, the related corporation will be taken to have collected the personal information for the same primary purpose as the first corporation. This will ensure that, unless one of the exceptions listed in APP 6 applies, the related corporation will have to

obtain the individual's consent before using or disclosing his or her personal information for a secondary purpose.

APP 6.7 provides that APP 6 will not apply to the use or disclosure of personal information for the purposes of direct marketing or to government related identifiers because these matters are dealt with elsewhere in the APPs.

Australian Privacy Principle 7—direct marketing

Direct marketing involves communicating directly with a consumer to promote the sale of goods and services to the consumer. The direct marketing communication could be delivered by a range of methods including mail, telephone, email or SMS. Direct marketers compile lists of consumers and their contact details from a wide variety of sources, including public records, the white pages, the electoral roll, registers of births, deaths and marriages and land title registers. They also include membership lists of business, professional and trade organisations, survey returns and mail order purchases.

Direct marketing is addressed separately within a discrete principle rather than as a kind of secondary purpose (see APP 6) because of the significant community interest about the use and disclosure of personal information for the purposes of direct marketing.

APP 7 will prohibit direct marketing by organisations.

Agencies will generally be exempt from the prohibition as it would impact on their ability to communicate legitimate and important information to individuals. However, a note to APP 7.1 draws attention to section 7A of the Privacy Act, which provides that an act or practice of an agency may be treated as an act or practice of an organisation if the agency engages in commercial activities. This means that the prohibition against direct marketing will also apply to agencies engaging in commercial activities.

APP 7 contains a distinction between individuals, such as existing or previous customers, who have been in contact with an organisation, and those who have not. However, the principle will not use terms such as 'customer' or 'non-customer'. Instead, it will capture the distinction by referring to individuals from whom an organisation has collected information and individuals from whom it has not. The intention is to apply more stringent obligations when using personal information of non-existing customers as the individual is less likely to expect their information to be used or disclosed for direct marketing purposes.

APPs 7.2 to 7.5 list exceptions to the rule against direct marketing. Under APP 7.2, an organisation may use or disclose personal information (other than sensitive information) for direct marketing if: the organisation collected the information from the individual; the individual would reasonably expect the organisation to use the information for direct marketing; the organisation has provided a simple means by which the individual can request not to receive direct marketing; and the individual has not availed him or herself of this means.

This exception will reflect the policy of requiring organisations to allow consumers to opt out of direct marketing. An opt-out rather than opt-in requirement is appropriate where the individual has provided the information to the organisation.

In the circumstances where the organisation has not obtained personal information from the individual, then opt-out still applies but there are additional requirements with respect to ensuring the individual is informed of their rights and how to exercise these rights.

Under APP 7.3, in cases where the individual would *not* reasonably expect his or her personal information to be used for direct marketing or the information has been collected from a third

party (so that, again, the individual would not reasonably expect to receive direct marketing from the organisation), the exception to the rule against direct marketing will be narrower. Under this provision, an organisation may use or disclose that information for direct marketing only if: the individual has consented (or it is impracticable to obtain consent); the organisation has provided the means to opt out and the individual has not opted out; and in each direct marketing communication the organisation must tell the individual that he or she may request to no longer receive direct marketing and no request is made.

Under APP 7.4, where an individual has provided *sensitive information* to an organisation, it will be necessary for the organisation to obtain the individual's consent before using that information for direct marketing purposes. There will be no provision that consent need not be obtained if doing so is impossible or impracticable, and it will not matter whether or not the individual and organisation have a pre-existing relationship.

Under APP 7.5, a contracted service provider for a Commonwealth contract may use or disclose personal information for the purposes of direct marketing if doing so meets an obligation under the contract. This provision will extend the general exemption of agencies from the rule against direct marketing to parties working for or on behalf of an agency.

APP 7.6 will provide that individuals may ask organisations who hold their personal information to stop sending direct marketing or to not disclose their personal information to other organisations for the purposes of direct marketing. They may also ask organisations to disclose their source of the information. Organisations must comply with such requests free of charge within a reasonable period. They need not comply with requests to disclose the source of information if it is impracticable or unreasonable to do so. The 'reasonable period' provisions will ease the compliance burden on organisations.

APP 7.6 applies to organisations that either use or disclose personal information for the purposes of direct marketing, or for the purpose of facilitating direct marketing by other organisations.

APP 7.6(b) will capture organisations that collect personal information for the purpose of providing that information to another organisation to facilitate direct marketing by that other organisation. For example, this will include a situation where a company has personal information that it provides to a retailer, and the retailer then uses that personal information for the purpose of directly marketing its products.

However, it is not intended that APP 7.6(b) will apply to organisations such as mailing houses that are utilised by a first organisation to simply send out direct marketing material for those companies. If those types of service providers are APP entities, their handling of personal information would be subject to the APPs. This is distinct from the situation where an entity carries out direct marketing on behalf of the first organisation, by for example, actually conducting the door to door direct marketing on behalf of the first organisation.

APP 7.8 will provide that instruments such as the *Spam Act 2003*, which contain specific provisions regarding direct marketing, will displace the more general provisions under the principle. Thus APP 7 will be displaced where another Act specifically provides for a particular type of direct marketing or direct marketing by a particular technology, but will apply to organisations involved in direct marketing relating to electronic messages and other acts and practices not covered by such instruments.

Australian Privacy Principle 8—cross-border disclosure of personal information

APP 8 sets out a requirement for an APP entity that chooses to disclose personal information to overseas recipients to take such steps as are reasonable in the circumstances to ensure that

the overseas recipient does not breach the APPs. Along with section 16C, this APP implements the new accountability approach to cross-border disclosure of personal information. This is reinforced in the note at the foot of APP 8.1, which refers to section 16C (which will provide that in certain circumstances, an act done, or a practice engaged in, by an overseas recipient can be taken to be a breach of the APPs by the entity which disclosed the personal information to the overseas recipient).

The principle will aim to permit cross-border disclosure of personal information and ensure that any personal information disclosed is still treated in accordance with the Privacy Act. This is a change from NPP 9, which prohibits cross-border disclosure, subject to some exceptions. The principle will apply to agencies as well as organisations, which is also a significant difference from the existing Act.

Although APP 8 explicitly adopts the term 'disclosure' rather than 'transfer', the APP 8 (and related provisions) would not apply to the overseas movement of personal information if that movement is an internal use by the entity, rather than a disclosure. APP 8 will apply where an organisation sends personal information to a 'related body corporate' located outside Australia.

It is not intended to apply where personal information is routed through servers that may be outside Australia. However, entities will need to take a risk management approach to ensure that personal information routed overseas is not accessed by third parties. If the information is accessed by third parties, this will be a disclosure subject to APP 8 (among other principles).

In terms of the reach of APP 8, the chain of accountability for APP entities would not be broken simply because the overseas entity engaged a subcontractor. For example, the requirements of APP 8 will still apply where an organisation contracts a function to an overseas entity (thereby making a cross border disclosure), and that overseas entity then engaged a subcontractor.

In practice, the concept of taking 'such steps as are reasonable in the circumstances' will normally require an entity to enter into a contractual relationship with the overseas recipient.

The general requirement to take reasonable steps to ensure compliance will be qualified by a number of exceptions:

- When the entity has a reasonable belief that the overseas recipient is subject to legal or binding obligations to protect information in at least a substantially similar way to the protection provided by the APPs, the requirement will not apply. For this exception to apply, there must be accessible mechanisms which allow the individual to enforce those protection obligations.

  The 'reasonable belief' test will allow entities to make decisions based on the information available to them and the context of a particular disclosure. The term 'substantially similar' will not be defined, and provides flexibility in considering the regulatory elements of the overseas jurisdiction. The term 'at least' will be used to ensure that stricter obligations than the APPs will still be compliant.

  It is not essential that the overseas jurisdiction have an office equivalent to the OAIC in order to provide accessible enforcement mechanisms. It should be possible for a range of dispute resolution or complaint handling models to satisfy this requirement. Effective enforcement mechanisms may be expressly included in a law or binding scheme or may take effect through the operation of cross-border enforcement

arrangements between the OAIC and an appropriate regulatory authority in the foreign jurisdiction.

- The requirement will not apply when an individual consents to the cross-border disclosure, after the entity informs the individual that the consequence of giving their consent is that the requirement in APP 8.1 will not apply.

  To reduce the compliance burden, this exception should not mean that consent is required before every proposed cross-border disclosure. Rather, it will apply where an individual has the explicit option of not consenting to certain disclosures which may include cross-border disclosures. In addition, an APP entity is required to give individuals notification about other entities to which the APP entity usually discloses personal information of the kind collected by the entity (APP 5.2(f)), and whether the APP entity is likely to disclose the personal information to overseas recipients (APP 5.2(i)).

- When the disclosure is required or authorised by or under law, the requirement will not apply.

- When some (but not all) permitted general situations exist (see Item 82), the requirement will not apply.

- When the disclosure is required or authorised by or under an international agreement relating to information sharing, the requirement will not apply if the entity is an agency and Australia is a party to the agreement. This is intended to include all forms information-sharing agreements made between an Australian and an international counterpart (for example, treaties, exchange of letters).

- When the entity is an agency, the requirement will not apply if the agency reasonably believes that the disclosure is reasonably necessary for enforcement related activities by, or on behalf of, an enforcement body and the overseas recipient's functions or powers are similar to those of an enforcement body. This is intended to enable an enforcement body to cooperate with international counterparts for enforcement related activities.

Australian Privacy Principle 9—adoption, use or disclosure of government related identifiers

The amended Act will include a definition of 'government related identifier' (see Item 23). Since government related identifiers are generally highly reliable for verification and identification of individuals, their use and disclosure will be addressed by more specific guidelines than the general 'use and disclosure' principle in APP 6.

APP 9 will regulate the adoption, use or disclosure of government related identifiers by organisations.

The principle will aim to restrict general use of government related identifiers by the private sector so that government related identifiers do not become universal identifiers, as well as to prevent data-matching by organisations facilitated by the use and disclosure of those identifiers.

The principle will prohibit an organisation from adopting a government related identifier to identify an individual unless that adoption is required or authorised by or under law or allowed under the regulations. The principle will also prohibit an organisation from using or

disclosing a government related identifier unless that use or disclosure falls within one of a list of specified exceptions. APP 9.2 will provide for exceptions relating to use or disclosure:

- where it is reasonably necessary to verify the identity of an individual for an organisation's activities or functions;
- where it is reasonably necessary to fulfil an organisation's obligations to an agency or State or Territory authority;
- where it is required or authorised by or under an Australian law, or a court/tribunal order;
- where some (but not all) permitted general situations exist (see Item 82);
- where an organisation reasonably believes is reasonably necessary for enforcement related activities by, or on behalf of, an enforcement body; and
- where it is allowed under the regulations.

These exceptions will recognise that balanced against the aims of the principle discussed above, there may be circumstances where use or disclosure of a government related identifier by an organisation may be necessary for public purposes or present a clear benefit to the individual. An example is to allow contracted service providers to use or disclose a government related identifier if necessary for the performance of a Commonwealth contract. The use of 'reasonably necessary' in a number of the exceptions will ensure that an objective test is applied.

The principle will allow for regulations to prescribe classes of organisations which may fall within the exception to the general prohibition on adoption, use and disclosure of government related identifiers. Allowing the regulations to prescribe classes of organisations is intended to reduce delays which may be caused by the requirement in the NPPs that individual organisations be prescribed. It will also reduce the need for continual updates to regulations, while still requiring clear articulation of the types of organisations that can interact with government related identifiers.

Part 4—Integrity of personal information

Australian Privacy Principle 10—quality of personal information

APP 10 sets out the obligation for an APP entity to take steps (if any) as are reasonable in the circumstances to ensure that the personal information it collects, uses and discloses meets certain quality requirements.

APP 10 is intended to ensure that personal information is accurate, up-to-date and complete. In relation to use and disclosure, the personal information should also be relevant and of a quality appropriate to the purposes of that use or disclosure. This will require entities to assess the relevance of personal information against the particular reason for its use or disclosure and only share so much of the personal information it holds as is relevant to that purpose. The quality assessment of personal information should occur at the time of collection, at the time of use and at the time of disclosure.

The requirements in APP 10.1 and 10.2 to 'take steps (if any) as are reasonable in the circumstances' will raise particular issues for information that might be out-of-date. For agencies, out-of-date information may become relevant for future activities (for example, prosecution of an individual for a criminal offence). In these circumstances, it may not be reasonable to update information, if it may, in its preserved form continue to be relevant into the future for a legitimate function or activity of the APP entity.

Australian Privacy Principle 11—security of personal information

APP 11 sets out an APP entity's obligations relating to the protection and destruction of personal information it holds.

The principle will require an entity to take such steps as are reasonable in the circumstances to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure. This should involve active measures by an entity to ensure the security of personal information.

The inclusion of 'interference' in APP 11 is intended to recognise that attacks on personal information may not be limited to misuse or loss, but may also interfere with the information in a way that does not amount to a modification of the content of the information (such as attacks on computer systems). This element may require additional measures to be taken to protect against computer attacks and other interferences of this nature, but the requirement is conditional on steps being 'reasonable in the circumstances'. Practical measures by entities to protect against interference of this nature are becoming more commonplace. The use of the term 'interference', which focuses on the result of the activity rather than the means used to achieve that result, ensures that the technologically neutral approach to the APPs is retained.

If an entity no longer needs personal information for any purpose for which it may be used or disclosed under the APPs, and if the information is not contained in a Commonwealth record or legally required to be retained by the entity, the principle will require that the entity destroy the information or ensure that it no longer meets the Privacy Act's amended definition of 'personal information'. This would require the entity to permanently remove from a record any information by which an individual may be identified, in order to prevent future re-identification from available data. Destruction should be proportional to the form of the record.

The principle will be flexible, in that the circumstances of each entity will determine when any personal information it holds is no longer necessary for any permitted purpose. The principle will in effect impose an obligation on entities to justify their retention of personal information.

Part 5—Access to, and correction of, personal information

Australian Privacy Principle 12—access to personal information

APP 12 provides that individuals must be granted access to personal information held about them by an APP entity upon request by the individual, subject to specific exceptions.

The principle will create separate exceptions for access to personal information held by agencies and organisations. This will reflect the responsibilities that agencies have under other Commonwealth legislation in relation to access to information, such as the *Freedom of Information Act 1982* (FOI Act). The right to access an individual's personal information held by an agency was also included in IPP 6. However, the FOI Act was treated as the principal avenue by which individuals were encouraged to seek access to the personal information. It is intended that the FOI Act should continue to be the primary legislative vehicle by which individuals can seek access to their personal information where it is contained in documents held by agencies.

The ALRC's recommendations which relate to including an enforceable right of access to, and correction of, an individual's own personal information in the Privacy Act (rather than maintaining the right through the FOI Act) will be considered at a later date.

In relation to organisations, APP 12.3 will create a number of exceptions which largely replicate NPP 6.1. The principle will combine the two 'serious threat' exceptions to remove the requirement that a threat be 'imminent', creating consistency with other sections of the Privacy Act (see Item 82).

The other exceptions relate to where:

- access would have an unreasonable impact on the privacy of other individuals;
- the request is frivolous or vexatious;
- the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings;
- giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations. This is intended to operate the same way as current NPP 6.1(f). An entity would not have to provide access to an individual's information if it would show the organisation's intentions and would prejudice or interfere in negative way in the organisation's negotiations with the individual (including where the negotiations are yet to commence but are reasonably anticipated);
- giving access would be unlawful, or denying access is required or authorised by or under an Australian law or a court/tribunal order;
- the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, or is being or may be engaged in, and giving access would be likely to prejudice the taking of appropriate action in relation to the matter;
- access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or
- access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

If an APP entity refuses to give an individual access to their personal information due to one of the exceptions, or in the manner requested, APP 12.5 will require the entity to take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the individual and the entity. This will ensure that entities work with individuals to try to satisfy their request.

Under APP 12.4, there are requirements for responding to the request within a certain timeframe and giving access to the information in the manner requested, if reasonable and practicable to do so. For organisations, they must respond to a request for access to personal information within a reasonable period after the request is made. It is intended that a 'reasonable period' under APP 12.4 relating to more complicated requests will not usually exceed 30 days.

The principle will provide for the possibility of alternative access through the use of a mutually agreed intermediary. This will reflect a strengthening of the obligation under NPP 6.3 to 'consider' the use of a mutually agreed intermediary.

Under APP 12.8, an organisation that charges an individual for providing access to the individual's personal information must ensure that the charges are not excessive and must not

apply to the making of the request. An excessive charge amount would include recouping costs above the actual amount incurred by the organisation.

If an APP entity refuses access to an individual's personal information due to one of the exceptions, or in the manner requested, APP 12.9 will also require the entity to give written reasons for the refusal. Written reasons will not be required, though, to the extent that it would be unreasonable with regard to the grounds for the refusal.

APP 12.10 provides that, if an APP entity refuses to give access to the personal information because of paragraph 12.3(j), the reasons for the refusal may include an explanation for the commercially sensitive decision. APP 12.10 will operate in the same manner as the repealed NPP 6.2 that enabled an organisation to provide an explanation for a commercially sensitive decision rather than direct access to the information.

Australian Privacy Principle 13—correction of personal information

APP 13 will set out the obligation for an entity to take reasonable steps to correct the personal information it holds about an individual if it is satisfied that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, with regard to the purpose for which it is held, or upon request by the individual. This obligation may include making appropriate deletions or additions.

The principle is not intended to create a broad obligation on entities to maintain the correctness of personal information it holds at all times. The principle will interact with APP 10, such that when the quality of personal information is assessed at the time of use or disclosure, an entity may need to correct the information before use or disclosure if the entity is satisfied that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading.

If personal information is held for a range of purposes, and it is considered incorrect with regard to one of those purposes, the obligation to take reasonable steps to correct the information should apply.

The principle will remove the requirement in NPP 6.5 for an individual to 'establish' that personal information is incorrect before correction is required.

If an entity corrects the personal information of an individual, APP 13 will require it to take reasonable steps to notify any other entity to which it had previously disclosed the information, if that notification is requested by the individual. The compliance burden will be reduced by the proviso that notification is not required if it would be impracticable or unlawful.

If an entity refuses to correct personal information in response to an individual's request, the principle will provide a mechanism for individuals to request that a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading be associated with the information. The entity must take reasonable steps to associate the statement so that it is apparent to users of the personal information. This will ensure that individuals retain control of how their personal information is handled. The statement should address matters relevant to the information being inaccurate, out-of-date, incomplete, irrelevant or misleading, and should not be unreasonably lengthy. The appropriate content and length of any statement will depend on the circumstances of the case.

Under APP 13.5, there are requirements for responding to requests under APP 13 within a certain time frame. For organisations, they must respond to such requests within a reasonable period after the request is made. It is intended that a 'reasonable period' under APP 13.5 relating to more complicated requests will not usually exceed 30 days.

The ALRC’s recommendations relating to including an enforceable right of access to, and correction of, an individual's own personal information in the Privacy Act (rather than maintaining the right through the FOI Act) will be considered at a later date.

Schedule 2 – Credit Reporting

Introduction

Outline of this schedule

This schedule amends the provisions that deal with credit reporting in the Privacy Act. Various definitions are replaced and additional definitions inserted to deal with new terms, Part IIIA is replaced with a new Part IIIA. The new provisions provide clear rules for participants in the credit reporting system by identifying the flows of personal information in the system and ensuring that regulation is consistent with the APPs. However, the credit reporting provisions differ from the APPs by providing different or more specific regulation in relation to certain personal information in the credit reporting system.

Related amendments to insert new provisions dealing with APP codes and the CR code (which replaces the previous credit reporting code of conduct) are dealt with in schedule 3. Amendments to the powers and functions of the Commissioner in relation to credit reporting are dealt with in schedule 4. The amendments in schedule 1 to insert the APPs are also relevant. In general terms, the order and structure of the credit reporting provisions reflects the order and structure of the APPs and the understanding of the personal information life cycle captured by the APPs. More specifically, where relevant the credit reporting provisions are directly modelled on the APPs, but modified as necessary to deal with the particular regulatory requirements of the credit reporting system. There is also the issue of the relationship between the regulation of personal information by the APPs and the regulation of certain kinds of personal information by the credit reporting system. The credit reporting provisions that deal with credit reporting bodies completely replace the APPs in relation to the defined kinds of personal information in the credit reporting system. Credit providers that are also APP entities will be subject to both the credit reporting provisions as well as to some APPs in some circumstances in relation to the kinds of personal information in the credit reporting system. The relationship between the credit reporting provisions and the APPs is fully addressed in the provisions and is discussed further below.

Objective of the credit reporting system

The purpose of the credit reporting system is to balance an individual's interests in protecting their personal information with the need to ensure sufficient personal information is available to assist a credit provider to determine an individual's eligibility for credit following an application for credit by an individual. The credit reporting system provides an aid to credit providers in managing the risks of providing consumer credit to individuals. Only limited and defined kinds of credit related personal information (described further below) are permitted in the credit reporting system.

The credit reporting system in Australia has been a 'negative' reporting system. The main kinds of personal information permitted in the system were information about a credit provider having sought a credit report in relation to an applicant for credit, the amount of credit sought in the application, the individual's current credit providers (if any), and information about any credit defaults (a term that was specifically defined). The new provisions move to a 'more comprehensive' credit reporting system. This means a limited number of additional categories of credit related personal information are permitted in the credit reporting system, as set out below. The provisions do not establish a 'positive' credit reporting system. That is, the credit reporting system does not provide every piece of credit related personal information about an individual. Moving to a more comprehensive credit reporting system balances the privacy interests of the individual while providing sufficient

information for credit providers to make an assessment of credit risk when considering an individual's eligibility for credit.

The credit reporting provisions do not regulate the way in which credit related personal information about an individual is used by credit providers to assess the risk of providing credit to an individual. This is a decision for each credit provider to make in the circumstances of each case in the context of the commercial practice of the credit provider.

Credit providers supply certain credit related personal information into the credit reporting system by disclosing it to credit reporting bodies. Credit reporting bodies collect and handle the information supplied by credit providers to create a database of permitted credit related personal information about an individual. The credit related personal information in the credit reporting system may be disclosed to other credit providers in defined circumstances. The credit reporting provisions place obligations on all participants in the credit reporting system. It is not mandatory for credit providers to participate in the credit reporting system, but if a credit provider chooses to participate they must comply with the credit reporting provisions as set out in the legislation and supported by regulations and the registered CR code. The credit reporting provisions do not deal with commercial arrangements that may be put into place between credit reporting bodies and credit providers. Matters of industry practice can be addressed by contractual arrangements or additional industry agreements that sit alongside the CR code. Industry agreements that may impact on competition in the credit reporting market would need to be considered by the Australian Competition and Consumer Commission.

An Australian credit reporting system

The credit reporting system is restricted to information about consumer credit in Australia and access to the credit reporting system is only available to credit providers in Australia. The credit reporting system will not contain foreign credit information or information from foreign credit providers (even if they have provided credit to an individual who is in Australia), nor will information from the credit reporting system be available to foreign credit reporting bodies or foreign credit providers.

One option considered to give effect to this policy was a number of general provisions stating these limitations. However, it was considered that a simpler, clearer and more effective approach was to ensure appropriate limitations were in place in relation to each relevant provision dealing with the collection, use and disclosure of information by credit reporting bodies and credit providers in Part IIIA. The key provisions are as follows. Clause 21D sets out a general prohibition on the disclosure of credit information by a credit provider to a credit reporting body (whether or not the body carries on business in Australia or not). This is followed by a permission to disclose credit information to a credit reporting body that has an Australian link. However, the provision specifies that the credit information that is disclosed must relate to credit that is or has been provided, or applied for, in Australia. Clause 20F, which sets out a table listing the permitted CRB disclosures that can be made, provides that (once the credit reporting body has collected this credit information) the credit reporting body can only disclose the credit information to a specified entity that also has an Australian link. Around these key provisions there are other provisions that contain appropriate limitations to ensure that relevant entities have an Australian link.

In this context, and consistent with the understanding of APP 8 on cross-border disclosures of personal information, online applications for credit submitted by an individual physically in Australia should be regarded as having been collected in Australia by the credit provider. Where the online application is made to a foreign entity, the foreign entity will not have an

Australian link and a credit reporting body will not be permitted to disclose credit reporting information to that foreign entity.

The concept of an Australian link is used in the APPs and is a term that is further defined in section 5B of the Act (as amended by schedule 4). It is understood that in the context of using this term in the credit reporting provisions, an entity with an Australian link should already have an appropriate link to Australia in place prior to any disclosure to that entity. The act of disclosure should not be what provides the entity with an Australian link.

Consideration will be given to the sharing of credit reporting information with New Zealand, which has a very similar credit reporting system and close economic ties with Australia. When this occurs, it will be necessary to develop specific legislative provisions to amend the credit reporting system set out in Part IIIA to establish the arrangements by which credit reporting information will be shared with New Zealand.

Main reforms to the credit reporting provisions

The credit reporting provisions have been completely revised, consistent with the intention to ensure greater logical consistency, simplicity and clarity throughout the Privacy Act. In addition to revisions to the credit reporting provisions, the major reforms of the credit reporting system are:

- Introducing more comprehensive credit reporting to provide additional information about an individual's ongoing credit arrangements:
    - Date credit account opened and date account closed (if any)
    - Type of credit
    - Maximum credit limit
    - Repayment history over previous two years
        - this category of information is only available to credit providers who are subject to responsible lending obligations under the *National Consumer Credit Protection Act 2009* (National Consumer Credit Protection Act)
        - however, there is an exception to this requirement for mortgage insurers to allow them to obtain the information from those credit providers to whom they provide mortgage insurance
- Reforming obligations relating to the retention of different categories of personal information
- Introducing specific rules to deal with pre-screening of credit offers and the freezing of access to an individual's personal information in cases of suspected identity theft or fraud
- Providing additional consumer protections by enhancing obligations and processes dealing with notification, data quality, access and correction, and complaints; and
- Reforming the regulation of credit reporting to more accurately reflect the information flows within the system and the general obligations set out in the APPs.

The credit reporting provisions will be supported by regulations and the registered CR code, which will deal with detailed and practical matters. In particular, the regulations and registered CR code will provide details on the information that can be collected as part of the new sets of information. The registered CR code will bind all credit reporting bodies. As it

is expected that the registered CR code will deal with certain matters as noted in the credit reporting provisions, it will also bind credit providers and other third parties who receive information from credit providers (such as the 'affected information recipients' dealt with in Division 4 of Part IIIA).

Participants in the credit reporting system

The credit reporting provisions apply to three main categories of participants: credit reporting bodies (formerly known as credit reporting agencies); credit providers; and affected information recipients, who are other third parties who receive the information from credit providers. The terms credit reporting bodies and credit providers are defined and have specific meanings. In general, a credit reporting body is a repository of the prescribed categories of personal information and does not have a direct relationship with the individuals to whom the information relates (however, a range of subsequent obligations, for example in relation to notification, access and correction, and complaints handling, will put a credit reporting body into direct contact with individuals). In general terms, a credit provider has a direct relationship with an individual through providing, or considering an application for the provision of, consumer credit (and, where permitted, commercial credit) to the individual.

The provisions dealing with each type of participant are grouped together, so that:

- Credit reporting bodies are dealt with in division 2
- Credit providers are dealt with in division 3; and
- Other recipients, known as affected information recipients (mortgage and trade insurers, related body corporate, credit managers, and advisors), are dealt with in Division 4.

A credit provider is permitted to disclose certain information to another credit provider in certain circumstances. It is recognised that this sharing of information is necessary to support the credit reporting system and sharing information in these circumstances does not make the credit provider subject to the obligations of a credit reporting body.

Categories of personal information in the credit reporting system

The credit reporting system only contains certain narrowly defined categories of credit related personal information. A number of general terms are used to refer to these categories of personal information. It is necessary to use a number of terms that incorporate and build upon other terms because it is essential to accurately describe the actual information flows in the credit reporting system. Generally, credit reporting bodies and credit providers that receive information out of the system use the information to determine some sort of credit score or rating of the credit risk of the individual which they add to the information. Because credit reporting bodies and credit providers may use personal information in the credit reporting system to derive and add new personal information to the system, it is important to accurately describe this process through the use of specific and defined terms. The key terms are: credit information; credit reporting information; credit eligibility information; and regulated information. These terms are discussed further, below.

Information flows into and out of the credit reporting system

There are two sides to the credit reporting system: the input side, by which credit providers put information into the system by disclosing the defined categories of personal information to credit reporting bodies; and the output side, by which credit reporting bodies disclose certain personal information to credit providers, where this is consistent with the permitted disclosures. While in this context it is useful to talk about information flows to understand

how the credit reporting system operates, all information flows are in fact comprised of a series of disclosures and collections of personal information, all of which are regulated by the credit reporting provisions.

In general terms, there will be a regular flow (disclosure) of information into the credit reporting system from credit providers to credit reporting bodies, as personal information about, for example, repayment history may be provided on a monthly basis. However, there is no automatic or continuous flow (disclosure) of information from credit reporting bodies to credit providers – information can only be disclosed in prescribed circumstances. Generally, information only comes out of the system following requests from credit providers to credit reporting bodies for disclosure for specified purposes (or where disclosures are permitted to certain recipients for certain purposes by operation of the provisions, such as to an affected information recipient, or where disclosure is permitted by operation of an exception, such as where a disclosure is required or authorised by or under an Australian law or court or tribunal order).

Diagram 1, below, provides a simplified illustration of the significant information flows in the credit reporting system. The key features of diagram 1 are as follows:

- The central circular relationship is between credit reporting bodies and credit providers.
    - Credit providers disclose 'credit information' to credit reporting bodies, which are the repositories of personal information in the credit reporting system.
    - Credit reporting bodies disclose 'credit reporting information' to credit providers.
- Credit reporting bodies may also disclose credit reporting information to:
    - 'mortgage insurers'
    - 'trade insurers'
    - 'securitisation entities'
    - in addition (and not included in the diagram for simplicity) credit reporting bodies may make a disclosure to another credit reporting body, a 'recognised external dispute resolution scheme', an 'enforcement body', as well as a disclosure that is required or authorised by or under an Australian law or court or tribunal order, or by regulations.
- Credit providers can disclose 'credit eligibility information' to:
    - other credit providers
    - 'affected information recipients'
    - in addition (and not included in the diagram for simplicity), credit providers can make a disclosure to a 'recognised external dispute resolution scheme', a 'guarantor', a 'debt collector', a mortgage credit assistance scheme, an 'enforcement body', as well as a disclosure that is required or authorised by or under an Australian law or court or tribunal order, or by regulations.

The use and disclosure of the types of personal information in diagram 1 are regulated, and are subject to conditions set out in the credit reporting provisions.

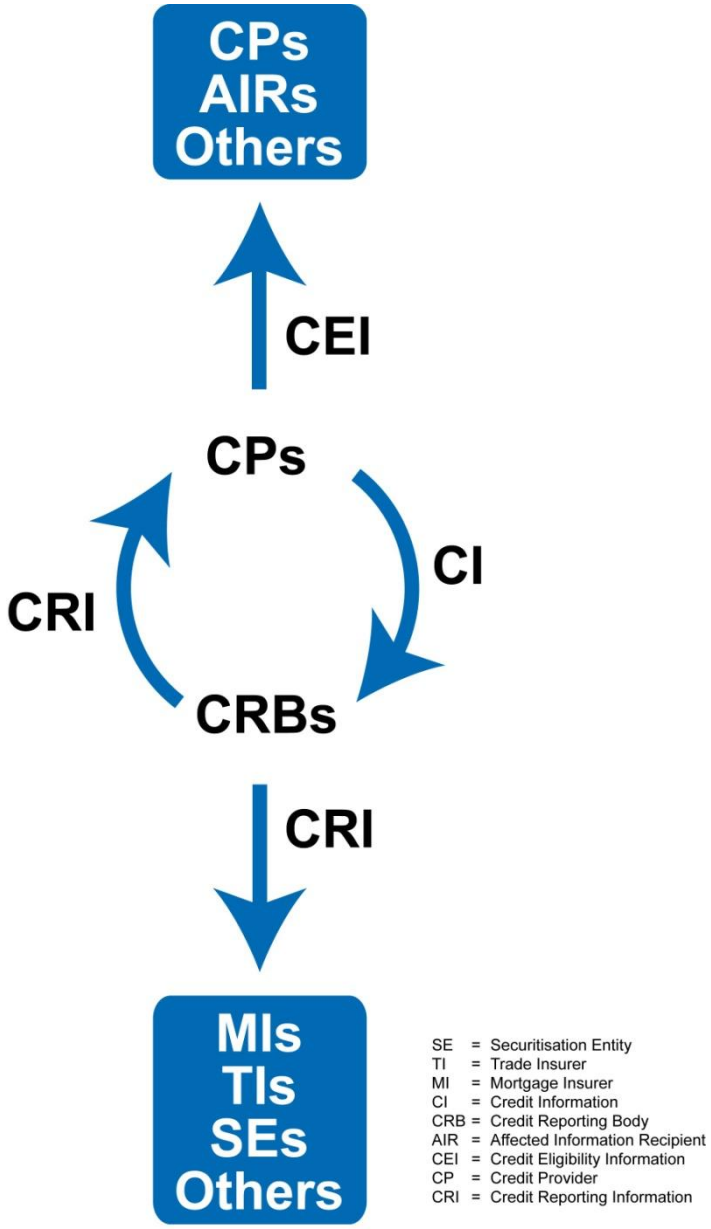

Diagram 1 – information flows in the credit reporting system

The credit reporting provisions provide different requirements for the participants based on whether they are taking part in the input side or the output side of the credit reporting system. This means that the rules for credit providers putting credit information into the credit reporting system are different to the rules that apply when they obtain credit reporting information from the credit reporting system. Credit providers have a dual role – they provide the credit reporting bodies with the personal information (credit information) necessary for the credit reporting system to operate, but their role on the output side of the system is to collect credit reporting information, which is personal information collected by the credit reporting body from other credit providers (if any) and any CRB derived information, which is personal information added by the credit reporting body, such as a credit score, assessment or other personal information about an individual that assists in determining an individual's credit worthiness.

This means, for example, that there can't be a single disclosure rule for credit providers, both because they have different roles in the system and because the personal information changes as it goes through the system. For this reason, there are provisions relating to the disclosure by credit providers to credit reporting bodies of credit information into the credit reporting system (and a related rule for credit reporting bodies dealing with collection of credit information). However, there are separate provisions relating to the disclosure by credit reporting bodies to credit providers, since the personal information disclosed will be credit reporting information. There are further provisions relating to any disclosures by credit providers of credit eligibility information. Credit eligibility information consists of credit reporting information disclosed to the credit provider by a credit reporting body, and CP derived information, which is any personal information added by the credit provider that assists in determining an individual's credit worthiness. There is not one single category of personal information that can be regulated by a single rule that will apply in every case.

There are further rules dealing with other permitted disclosures by credit reporting bodies and credit providers. These disclosures are for specific purposes. Most recipients will be subject to further provisions in relation to their use of the personal information they have collected, as well as any further disclosure of the personal information. For example, 'authorised information recipients' are subject to the requirements set out in Division 4 in relation to 'regulated information'. Further disclosure by these authorised information recipients is prohibited. The credit reporting provisions do not specifically deal with personal information that is held or maintained by: a recognised external dispute resolution scheme; an enforcement body; or a debt collector. An enforcement body will be an APP entity, and, if the other recipients are also an APP entity, they will be subject to the APPs. A recipient who is a person who is a guarantor is likely to be an individual and exempt from the Act, while a mortgage credit assistance scheme is expected to be a State or Territory agency and exempt from the Act.

Key terms that refer to personal information in the credit reporting system

There are a number of definitions associated with the credit reporting provisions that provide explanations of the terms to assist understanding and ensure that only the precisely defined kinds of personal information are held in the credit reporting system. This is consistent with the prescriptive nature of the credit reporting system. Many of these definitions are linked. This reflects the way in which personal information in the credit reporting system is maintained and used. In particular, both credit reporting bodies and credit providers use the personal information they collect to derive their own assessments of the individual's credit worthiness. In this context, it is understood that to derive means to use the personal information to determine some sort of credit score or rating (or other relevant personal information) that usually relates to the perceived credit risk of the individual for the purpose of considering the individual's credit worthiness. The aggregation of personal information in this way gives credit providers a better understanding of an individual's credit worthiness. In the same way that the different kinds of personal information in the credit reporting system are pulled together, the definitions of terms used to refer to those kinds of personal information must also be linked rather than stand alone. Despite the number of specific definitions of terms that are used in the credit reporting provisions, only four key terms deal with the accumulation of relevant personal information through the information flows that make up the credit reporting system.

Diagram 2, below, provides a simple illustration of the relationship of the key terms to the information flows in the credit reporting system, as well as their relationship to credit providers, credit reporting bodies and authorised information recipients. For simplicity,

diagram 2 does not represent all the information flows in the credit reporting system (as set out in diagram 1). The credit reporting provisions set out the circumstances in which the different types of personal information can be collected, used or disclosed.

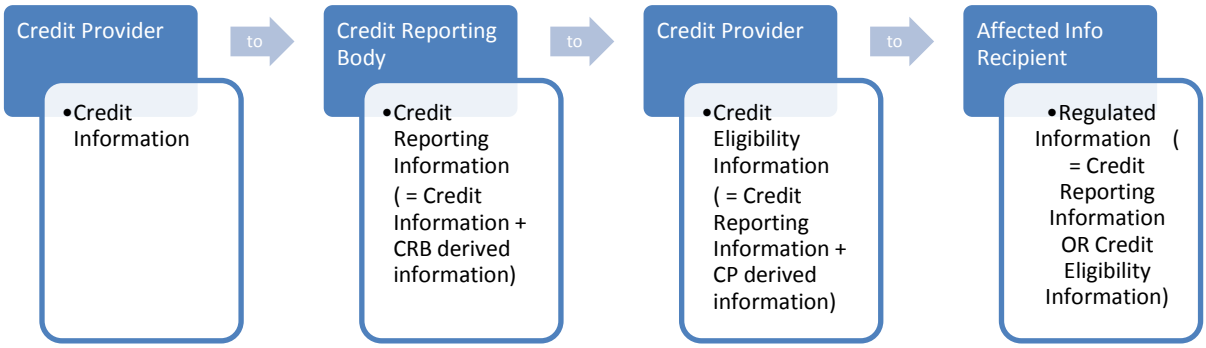

Diagram 2 – key terms that refer to personal information in the credit reporting system

(a) credit information

Credit information is the basic category of personal information in the credit reporting system. The term credit information brings together a defined list of certain kinds of personal information that are relevant to the credit reporting system. However, any information that would fall within the definition of sensitive information in the Act is expressly excluded from credit information. The following types of personal information included in the definition of credit information are also separately defined: identification information; consumer credit liability information; repayment history information; information requests, as well as information about the type and amount of credit sought in the application; default information; payment information; new arrangement information; court proceedings information; and personal insolvency information. The five new types of personal information that comprise the more comprehensive credit reporting reforms are captured as part of consumer credit liability information and repayment history information. In addition, credit information includes two other types of personal information: information about certain publicly available information about the individual that relates to the individual's activities in Australia and their credit worthiness; and information that is the opinion of a credit provider that the individual has committed a serious credit infringement (which is itself a defined term).

(b) credit reporting information

Credit reporting information = credit information + CRB derived information

Credit reporting bodies hold and maintain credit reporting information. Credit providers collect credit information from individuals who apply for credit. This credit information is disclosed to credit reporting bodies that compile the credit information about an individual collected from credit providers. Credit reporting information consists of two categories of personal information; the credit information about an individual that was disclosed to the

credit reporting body by credit providers; and CRB derived information. CRB derived information means any personal information about an individual (that is not sensitive personal information) that the credit reporting body derives from the credit information about the individual held by the credit reporting body. However, the personal information must have some bearing on the individual's credit worthiness and be used to establish the individual's eligibility for consumer credit.

(c) credit eligibility information

Credit eligibility information = credit reporting information + CP derived information

Credit providers hold and maintain credit eligibility information, which is the final product of the flow of credit information through the credit reporting system. Credit reporting bodies disclose credit reporting information to credit providers in defined circumstances. A credit provider that receives credit reporting information generally performs its own analysis of that information in relation to the individual's credit worthiness. This is CP derived information – personal information (which cannot include sensitive information) derived from the credit reporting information provided to the credit provider which has some bearing on the individual's credit worthiness and can be used to establish the individual's eligibility for consumer credit. Credit eligibility information consists of the credit reporting information provided to the credit provider by the credit reporting body and the CP derived information.

(d) regulated information

Regulated information = credit eligibility information or credit reporting information

An affected information recipient is a term used to refer to certain entities or persons that may be (apart from trade insurers) provided with credit eligibility information in certain circumstances. Where the affected information recipient is a mortgage insurer, they may also be provided with credit reporting information by a credit reporting body in certain circumstances. Where the affected information recipient is a trade insurer, they may be provided with credit reporting information by a credit reporting body in certain circumstances. The term regulated information refers to these types of personal information in the hands of the affected information recipient, and in relation to which certain obligations are imposed. The circumstances in which disclosures can be made to affected information recipients are narrowly prescribed. The term 'affected information recipients' refers to a variety of entities or persons, and these entities and persons are subject to obligations in relation to their privacy policy, to provide notice to individuals about certain matters, and in relation to the use and disclosure of regulated information.

Relationship of credit reporting provisions to the APPs

The credit reporting provisions that apply to credit reporting bodies completely replace the APPs in relation to the types of personal information to which they apply. However, the provisions for credit providers take a different approach. The credit reporting provisions apply to all credit providers (and, in special cases, to other entities or persons, such as those entities or persons that fall within the definition of an affected information recipient) in relation to the types of personal information to which they apply. In addition, those credit providers that are also APP entities may also be subject to some APPs depending on the circumstances. Provisions have been inserted to clarify the relationship of particular credit reporting provisions to the APPs. Each provision in Division 3 on credit providers that deals with matters that are also covered by one or more of the APPs contains a provision that clarifies the relationship of that provision with the relevant APPs. In most cases, the provision makes clear that the credit reporting provision replaces the relevant APP in relation to the particular kind of personal information that is regulated. This difference in approach is

due to the very different roles of the parties in the credit reporting system. Credit reporting bodies are central to the system and require rules that apply to every aspect of the system. However, credit providers take part in the credit reporting system for the purpose of providing or managing credit, and their primary obligations in relation to personal information are established by the APPs. For credit providers, the credit reporting rules apply over the top of the APPs in relation to the kinds of personal information regulated in the credit reporting system. In relation to all other kinds of personal information the APPs will apply.

Access, correction and complaints procedures

Specific access, correction and complaints provisions set out obligations of credit reporting bodies and credit providers. The main feature of these provisions is that a credit reporting body or a credit provider that receives a correction request from the individual is, where necessary, required to undertake appropriate consultations with other credit reporting bodies or credit providers to assist in resolving the correction request. Consultations will be necessary where the body or provider that receives the correction request does not itself hold the relevant information nor have evidence supporting the information. It will be necessary for credit reporting bodies and credit providers to develop appropriate systems to ensure that correction requests are dealt with quickly and efficiently. In addition, a substantiation obligation is imposed where a correction request is refused. This means that evidence must be provided to the individual demonstrating the accuracy of the information for which correction has been refused. Finally, obligations around complaints have been developed to ensure that individuals are informed of their options to lodge a complaint with an approved external dispute resolution service or with the Commissioner, using the procedures set out in Part V of the Act.

Civil penalties and offences

There was previously a number of credit reporting offences (criminal offences) in relation to the credit reporting provisions. These provisions have been removed and replaced with civil penalty provisions were appropriate. However, where the nature of the conduct that is to be prohibited justifies an offence provision, such provisions have been inserted - see clauses 20P and 21R in relation to the use and disclosure of false and misleading information and clauses 24 and 24A in relation to the unauthorised obtaining of information from a credit reporting body or credit provider. In each case, civil penalty provisions have also been inserted in relation to the same conduct. The insertion of both offences and civil penalties allows the appropriate remedy to be sought depending on the particular circumstances of each case.

Transitional arrangements

Transitional arrangements are set out in schedule 6. Of particular relevance to the credit reporting provisions is the proposed capture of repayment history information prior to commencement. On commencement credit providers will be permitted to disclose to credit reporting bodies repayment history information dating back to the date of Royal Assent. As the commencement period will be 9 months, this means that credit providers will be able to disclose approximately 9 months of repayment history information. The purpose of permitting this arrangement is to provide a meaningful amount of data on repayment history from the commencement of the new credit reporting system.

Credit reporting information that has been de-identified

De-identified information is not a defined term. However, credit reporting information held by credit reporting bodies that is de-identified is subject to specific regulation by clause 20M. The de-identification of personal information as an alternative to destruction is an option

provided in the APPs, and credit providers are also permitted to de-identify credit information or credit eligibility information by the credit reporting provisions. However, when credit reporting bodies de-identify credit reporting information, the use and disclosure of that information by credit reporting bodies is regulated.

Notes on Clauses

Item 1 Before section 6

This item inserts the Division heading for the general definitions.

Item 2 Subsection 6(1)

This item inserts a cross-reference to the definition of *access seeker* in subclause 6L(1).

Item 3 Subsection 6(1)

This item inserts the definition of *affected information recipient*. The term 'affected information recipient' has been used to refer collectively to a number of different entities or persons to whom certain personal information is disclosed (known as 'regulated information') by credit reporting bodies or credit providers in certain circumstances set out in Divisions 2 and 3. Division 4 contains provisions dealing with the handling of 'regulated information' by affected information recipients. An affected information recipient is a mortgage insurer, a trade insurer, a related body corporate of a credit provider (as referred to in paragraph 21G(3)(b)), a person who manages credit provided by a credit provider (as referred to in paragraph 21G(3)(c)), or an entity or a professional legal adviser or professional financial adviser for the entity (as referred to in paragraph 21N(2)(a)) to whom the credit provider discloses credit eligibility information for certain purposes dealing with assignment of debts, acceptance of debts, or purchasing an interest in the provider.

Item 4 Subsection 6(1)

This item inserts a cross-reference to the definition of *amount of credit* in subclause 6M(2).

Item 5 Subsection 6(1)

This item clarifies that a reference to the Bankruptcy Act means the *Bankruptcy Act 1966*.

Item 6 Subsection 6(1)

This item inserts a cross-reference to the definition of *ban period* in subclause 20K(3).

Item 7 Subsection 6(1) (definition of *commercial credit*)

This item repeals the existing definition of commercial credit and inserts a new definition of *commercial credit*. The term 'commercial credit' is used in other definitions, including the definition of 'trade insurance purpose' (see item 64) and 'trade insurer' (see item 65).

'Commercial credit' is any credit other than consumer credit that is applied for, or provided to, a person. This means that any credit that is not 'consumer credit' is, for the purposes of the credit reporting provisions, taken to be commercial credit. Note that the definition of 'consumer credit' has been expanded to include credit obtained to acquire, maintain, renovate or improved residential property for an investment purposes or to refinance consumer credit provided for this purpose. This means that credit obtained for residential property investment purposes (that satisfies the criteria set out in the definition of 'consumer credit') is not commercial credit.

Item 8 Subsection 6(1)

This item inserts a definition of *commercial credit related purpose*. This definition is linked to the term 'commercial credit'. Credit reporting bodies may disclose credit reporting information to a credit provider where the provider requests the information for a commercial credit related purpose (see subclause 20F(1)) and the individual expressly consents to the disclosure. Where the relevant credit reporting information was disclosed to the credit provider for a commercial credit related purpose, the credit provider can then use the credit

eligibility information for that purpose (see subclause 21(H)). A credit provider can also disclose credit eligibility information to another credit provider for a commercial credit related purpose (see subclause 21J(1)) and the individual expressly consents to the disclosure.

A credit provider has a commercial credit related purpose in relation to a person if the purpose is to assess an application for commercial credit made by that person to the provider, or to collect payments that are overdue in relation to the commercial credit provided by the provider to that person.

Item 9 Subsection 6(1)

This item inserts the definition of *consumer credit*. This definition is, along with the definition of 'credit worthiness', central to the purpose of the credit reporting system, which is established to allow credit providers to use certain personal information to determine an individual's 'credit worthiness' and establish the individual's eligibility for consumer credit.

The definition of 'consumer credit' has two parts. Consumer credit is credit for which an individual has made an application to a credit provider, or credit that has been provided to an individual by a credit provider, in the course of the credit provider carrying on a business or undertaking as a credit provider. In addition, the credit that is applied for or which is provided must be intended to be used wholly or primarily for certain purposes. These purposes are: for personal, family or household purposes; to acquire, maintain, renovate or improve residential property for investment purposes; or to refinance consumer credit that has been provided wholly or primarily to acquire, maintain, renovate or improve residential property for investment purposes.

Any credit that does not fall within this definition is 'commercial credit'.

The term 'consumer credit' replaces the former definition of 'credit'. The credit reporting provisions have, from their insertion into the Act, applied to credit that an individual intends to use wholly or primarily for personal, family or household purposes. However, the definition has now been broadened to include credit obtained for the purposes of investing in residential property and related purposes as set out in the definition. Extending the application of the credit reporting system to these credit transactions is consistent with the National Consumer Credit Protection Act, which protects these types of credit transactions. Formerly, credit transactions in relation to residential property for investment purposes would have been considered commercial credit transactions. However, extending the protection of NCCP Act to these types of credit transactions recognised that consumers formed a significant segment of the residential investment property credit transactions. Accordingly, it is appropriate to extend the definition of consumer credit to ensure that the personal information of individuals undertaking these transactions is also adequately protected by the credit reporting provisions.

Item 10 Subsection 6(1)

This item inserts the definition of *consumer credit liability information*. The term 'consumer credit liability information' comprises one of the most significant parts of an individual's 'credit information' (see clause 6N). 'Consumer credit liability information' sets out the important information about an individual's credit obligations. Previously, in relation to the description of the individual's credit obligations, only the name of an individual's credit provider was permitted to be included as part of the individual's personal information in the credit reporting system. This definition now permits certain other types of information to be included along with the credit provider's name. These types of information are four of the new types of personal information about an individual that are permitted in the move to a

more comprehensive credit reporting system. The fifth new type of information, repayment history information, is separately defined.

The definition of 'consumer credit liability information' refers to certain information about the consumer credit that a credit provider provides to an individual. Any information about an individual's commercial credit cannot be included in an individual's consumer credit liability information. The definition sets out the types of information that can be included as consumer credit liability information, as follows.

The name of the credit provider allows identification of the credit provider that provides consumer credit to an individual, so that, for example, written notes of disclosures by credit reporting bodies can clearly identify the credit provider to which credit reporting information has been disclosed.

Whether the credit provider is a licensee is also included in the definition. 'Licensee' is defined to have the meaning given to the term by the NCCP Act. Inclusion of this information is necessary to determine to which credit providers repayment history information can be disclosed. Repayment history information can only be disclosed to credit providers who are licensees. This is because licensees are subject to responsible lending obligations under the NCCP Act, and the repayment history information is intended to assist those credit providers meet those obligations. If it is not clear from an individual's consumer credit liability information that a credit provider is a licensee, then repayment history information about that individual should not be disclosed to that credit provider.

The type of consumer credit provided to the individual is included in the definition. It is expected that the registered CR code will set out common descriptors for use in describing different types of consumer credit. This is not intended to be a detailed description of the circumstances around the provision of credit. While a general description of the type of credit is permitted, it is expected that the description will provide sufficient information to be useful for establishing an individual's credit worthiness – for example, mortgage credit is a different type of credit to credit provided for residential property investment.

The day on which the consumer credit was entered into is included in the definition. It is expected that this will generally refer to the date on which the contract for consumer credit was entered, although it is expected the registered CR code will provide more details about this category – for example, if a contract is not signed immediately but the credit is supplied, it is expected that the day on which the consumer credit was entered into would generally be the day the credit was available to the individual.

The definition of 'consumer credit liability information' includes the terms or conditions of the consumer credit that relate to the repayment of the amount of credit. However, this personal information can only be included where it is prescribed by the regulations. If no regulations are made setting out the appropriate terms and conditions that are permitted, then no information about these matters can be included as part of an individual's consumer credit liability information. The terms and conditions of an individual's consumer credit are likely to be many and varied. Only those terms and conditions that would assist in determining an individual's credit worthiness are intended to be included. In this regard the regulations may prescribe matters such as, for example, whether the credit is repaid by interest only or by principal and interest, whether the interest rate is fixed or variable, and whether the credit is secured or unsecured. These matters, if included in regulations, would provide more information to assist understanding the type of consumer credit provided to the individual and, more generally, along with the other information included in the definition of consumer credit liability information, the nature of an individual's consumer credit liabilities. The

registered CR code may also provide more information on this the terms or conditions to be included.

The maximum amount of credit available under the consumer credit is included in the definition. This does not refer to the day-to-day balance for an individual's credit account. The maximum amount of credit indicates how much credit is available to the individual, but does not indicate whether the individual has used all the credit available. Different credit products may supply credit in different ways and it may not be straightforward to determine the maximum credit available. It is expected that the registered CR code will provide guidance on how the maximum amount of credit available is to be determined.

The day on which the consumer credit is terminated or otherwise ceases to be in force is the final type of information included in the definition. This refers to the day the consumer credit is no longer available to the individual because the consumer credit has been terminated or otherwise ceases to be in force, not to the day the individual has, for example, made the last repayment on consumer credit (unless in the circumstances the day of the last repayment means that the consumer credit ceases to be in force). Depending on the type of consumer credit, in some circumstances the individual may continue to have access to the credit after repaying the credit. This means that the consumer credit would not be taken as terminated until the individual no longer had access to the credit. Credit providers should clearly indicate to consumers the circumstances in which their credit will be terminated or otherwise ceases to be in force, and whether the consumer must take any action in addition to making the final repayment to terminate the credit or for it to otherwise cease to be in force. There may be other circumstances in which the credit is terminated or otherwise ceases to be in force – for example, the individual does an act that is a serious credit infringement. The date that the consumer credit is terminated or otherwise ceases to be in force is necessary to calculate retention periods for consumer credit liability information and other credit reporting information about the individual. It is expected that the registered CR code will provide additional guidance on determining the day on which consumer credit is terminated and the other circumstances in which the consumer credit ceases to be in force.

Item 11 Subsection 6(1)

This item inserts the definition of *consumer credit related purpose*. This term is linked to, and should be read with, the definition of 'consumer credit'. Credit reporting bodies can disclose credit reporting information to credit providers where the provider request the information for a consumer credit related purpose under subclause 20F(1). Credit providers can use credit eligibility information for a consumer credit related purpose of the credit provider under subclause 21G(2). The use and disclosure of certain personal information for a consumer credit related purpose is central to the operation and purpose of the credit reporting system.

A consumer credit related purpose of a credit provider in relation to an individual means either the purpose of assessing an application for consumer credit made by the individual to the provider, or collecting payments that are overdue in relation to consumer credit provided by the provider to the individual.

The definition of consumer credit related purpose limits the purposes for which certain personal information may be uses or disclosed. The definition sets out the only permitted consumer credit related purposes. It would not be consistent with the definition for credit reporting bodies to disclose credit reporting information about an individual to credit providers on a regular or continuous basis. Rather, the credit provider is required to separately request the credit reporting body to disclose the relevant personal information on

each occasion where the credit provider wishes to collect that personal information. While a credit provider is permitted to use credit eligibility information for the purpose of assisting an individual to avoid defaulting (see clause 21H), it is expected that the use for this purpose would only be necessary when the provider has a basis for believing that the individual may be at risk of defaulting. It would not be consistent with the definition of consumer credit related purpose for the provider to obtain regular disclosures from the credit reporting body simply to monitor or check an individual's overall credit worthiness or behaviour.

Item 12 Subsection 6(1)

This item inserts the definition of *court proceedings information*. Information about court proceedings that is held and maintained as part of an individual's 'credit information' (see clause 6N) must be directly related to credit. It is not permissible for information about any criminal law matters to be included in an individual's credit information, nor for information about any other matters, such as commercial or civil law matters, unless the matter is related to the credit provided to, or applied for, by the individual.

This provision only permits information about a judgement of an Australian court - no foreign court information is permitted. The judgement must be made, or given, against the individual in proceedings, and the judgement must relate to any credit provided to, or applied for, by the individual.

The definition expressly refers only to judgments, not any other form of, or stages in, court proceedings. This means that, for example, an originating summons cannot be included in an individual's credit information as court proceedings information because it is not a judgement (even though it is part of the proceedings of the court).

Item 13 Subsection 6(1)

This item inserts the definition of *CP derived information*. CP derived information is any personal information about an individual that is derived from credit reporting information that was disclosed to the credit provider by a credit reporting body under Division 2. In addition, to be CP derived information the personal information must be information that has any bearing on the individual's 'credit worthiness', and be used (or has been used, or could be used) to establish the individual's eligibility for 'consumer credit'.

To derive information from other information (the source information) is to obtain or deduce other personal information from the source information. It is secondary information in that it is not possible for a credit provider to produce CP derived information without first having the source information about the individual (in this case, the source information is credit reporting information) to form the basis for the derivation process. Generally, it is understood that CP derived information will include a credit rating or score that has a bearing on the individual's credit worthiness by indicating the provider's analysis of the individual's eligibility for consumer credit. A provider is not limited to using only credit reporting information to derive for CP derived information, but may also use other information together with credit reporting information to derive CP derived information about the individual (such as, for example, the provider's risk analysis that takes into account other economic or commercial factors).

CP derived information cannot be 'sensitive information' as defined in section 6(1). This prohibition applies to all forms of sensitive information as set out in the definition of that term. While, under the APPs, APP entities can generally collect sensitive information with the consent of the individual, this provision makes clear that sensitive information is prohibited in the credit reporting system. To ensure this is the case it is expected that sensitive information cannot form a part of the information used by a credit provider to derive

CP derived information about an individual, or be considered in any way by a provider in CP derived information.

Item 14 Subsection 6(1)

This item inserts the definition of *CRB derived information*. CRB derived information is personal information about an individual derived by a credit reporting body from credit information about the individual that is held by the credit reporting body. In addition, to be CRB derived information it must have some bearing on the individual's 'credit worthiness', and be used (or has been used, or could be used) to establish the individual's eligibility for consumer credit.

To derive information from other information (the source information) is to obtain or deduce other personal information from the source information. It is secondary information in that it is not possible for a credit reporting body to produce CRB derived information without first having the source information about the individual (in this case, the source information is credit information) to form the basis for the derivation process. Generally, it is understood that CRB derived information will include a credit rating or score that has a bearing on the individual's credit worthiness by indicating the body's analysis of the individual's eligibility for consumer credit. A body is not limited to using only credit information to derive for CRB derived information, but may also use other information together with credit information to derive CRB derived information about the individual (such as, for example, the body's risk analysis that takes into account other economic or commercial factors).

CRB derived information cannot be 'sensitive information' as defined in section 6(1). This prohibition applies to all forms of sensitive information as set out in the definition of that term. While, under the APPs, APP entities can generally collect sensitive information with the consent of the individual, this provision makes clear that sensitive information is prohibited in the credit reporting system. To ensure this is the case it is expected that sensitive information cannot form a part of the information used by a credit reporting body to derive CRB derived information about an individual, or be considered in any way by a provider in CRB derived information.

Item 15 Subsection 6(1) (definition of *credit*)

This item repeals the existing definition of *credit* and inserts a cross-reference to the new definition of 'credit' in subclauses 6M(1) and (3). The new definition of credit replaces the former definition of 'loan'. The definition of credit includes the term 'amount of credit' in subclause 6M(2).

Item 16 Subsection 6(1) (definition of *credit card*)

This item replaces any references to the term 'loans' in the definition of *credit card* with the term 'credit'. The term 'loans' has been repealed because this term has been replaced with 'credit'.

Item 17 Subsection 6(1)

This item inserts the definition of *credit eligibility information*. Credit providers hold and maintain credit eligibility information, which is personal information. Credit eligibility information comprises 'credit reporting information' that was disclosed to the provider by a credit reporting body and 'CP derived information'.

Credit reporting bodies disclose credit reporting information to credit providers in defined circumstances under Division 2. It is understood that a credit provider that collects credit reporting information performs its own analysis on that information and may use it (either

alone or together with other information) to derive further information about an individual's credit worthiness that can be used to establish the individual's eligibility for consumer credit. The personal information that results from this process is CP derived information. Credit eligibility information refers to these kinds of personal information about the individual held by the credit provider. The obligations of credit providers in relation to credit eligibility information are set out in Division 3.

The definition of credit eligibility information only includes credit reporting information disclosed to the credit provider by a credit reporting body. It does not include other credit-related information that was, for example, collected directly from the individual. That other credit-related information would not be subject to the credit reporting provisions (but, if the provider is an APP entity, would be subject to the APPs). In some instances a credit provider may collect the same information from different sources, for example from a credit reporting body and from the individual. In these circumstances, the credit provider will be required to distinguish between personal information that is credit eligibility information (collected from a credit reporting body) and other personal information they collect.

Item 18 Subsection 6(1) (definition of *credit enhancement*)

This item replaces the reference to the term 'a loan' in the definition of *credit enhancement* with the term 'credit'. The term 'loan' has been repealed because this concept has been replaced with 'credit'.

Item 19 Subsection 6(1) (paragraphs (a) and (b) of the definition of *credit enhancement*)

This item replaces the references to the term 'the loan' in the definition of *credit enhancement* with the term 'the credit'. The term 'loan' has been repealed because this concept has been replaced with 'credit'.

Item 20 Subsection 6(1)

This item inserts the definition of *credit guarantee purpose*. An individual may wish to act as guarantor for credit provided to another person. The individual may offer the guarantee either at the time the other person applies for the credit, or after the credit has been provided to the other person. An individual who offers to act as a guarantor is offering to take on consumer credit liabilities in relation to that credit applied for, or provided to, the other person.

A credit reporting body is permitted to disclose credit reporting information to a credit provider that requests the information for a credit guarantee purpose (see subclause 20F(1)). Where the relevant credit reporting information was disclosed to the credit provider for a credit guarantee purpose, the credit provider can then use the credit eligibility information for that purpose (see subclause 21(H)).

A credit guarantee purpose means the purpose of assessing whether to accept the individual as a guarantor for credit for which an application has been made to, or which has been provided by, a credit provider by a person other than the individual who is proposing to be a guarantor.

Item 21 Subsection 6(1)

This item inserts a cross-reference to the definition of *credit information* in clause 6N.

Item 22 Subsection 6(1) (definition of *credit information file*)

This item repeals the definition of *credit information file* as the term is no longer used. The concept of a file no longer accurately reflects the way personal information is held and maintained in the credit reporting system.

Item 23 Subsection 6(1) (definition of *credit provider*)

This item inserts a new cross-reference to the definition of *credit provider* in clauses 6G to 6K, as these clauses replace the previous definition of this term.

Item 24 Subsection 6(1) (definition of *credit report*)

This item repeals the definition of *credit report*, as the term is no longer used. The concept of a credit report no longer accurately reflects the way personal information is held or maintained in the credit reporting system.

Item 25 Subsection 6(1) (definition of *credit reporting agency*)

This item repeals the definition of *credit reporting agency* as it has been replaced by the term 'credit reporting body'.

Item 26 Subsection 6(1)

This item inserts the definition of *credit reporting body*, which replaces the previous definition of 'credit reporting agency'. The reference to 'agency' in the previous term has been replaced with 'body' to ensure that there is no confusion with Government agencies, particularly now that the definition provides for an agency to be a credit reporting body if it is prescribed by regulations. A credit reporting body is either an organisation that carries on a 'credit reporting business' or an agency prescribed by the regulations that carries on a 'credit reporting business' (as defined in clause 6P). A credit reporting body is subject to the obligations set out in Division 2.

It is not anticipated that any agencies will be prescribed by the regulations. However, this provision provides the option of prescribing an agency in the future if any agency is established as, or identified to be, a credit reporting body. An agency that is a credit reporting body will be subject to the same regulatory requirements as an organisation or small business operator that is a credit reporting body.

A credit reporting body that is a small business operator will be treated as an organisation for the purposes of the Act. The definition of 'organisation' in section 6C excludes a small business operator. However, subsection 6D(4) specifies certain entities that are not small business operators and hence which are treated as organisations. Item 68 amends subsection 6D(4) by adding an additional paragraph referring to a credit reporting body. This means that a credit reporting body that is a small business is not, for the purposes of the Act, a small business operator. It is appropriate that small business operators are permitted to be credit reporting bodies and play a role in the credit reporting system. However, those small business operators should be subject to the obligations in the Act that apply to other organisations, such as the APPs, and the obligations in the Act that apply to credit reporting bodies, in particular, the obligations set out in Part IIIA of the Act.

Item 27 Subsection 6(1) (definition of *credit reporting business*)

This item repeals the existing definition of *credit reporting business* and inserts a cross-reference to the new definition of 'credit reporting business' in clause 6P.

Item 28 Subsection 6(1)

This item inserts the definition of *credit reporting information*. Credit reporting bodies hold and maintain credit reporting information, which is personal information. Credit reporting information about an individual consists of 'credit information' that was disclosed to the credit reporting body by the credit provider, as well as 'CRB derived information'.

Credit providers collect credit information from individuals who apply for credit. This credit information may be disclosed in certain circumstances (under Division 3) to credit reporting bodies that compile the credit information about an individual collected from credit providers. It is understood that a credit reporting body that collects credit information performs its own analysis on that information and may use it (either alone or together with other information) to derive further information about an individual's credit worthiness that can be used to establish the individual's eligibility for consumer credit. The personal information that results from this process is CRB derived information. Credit reporting information refers to these kinds of personal information about the individual held by the credit reporting body. The obligations of credit reporting bodies in relation to credit reporting information are set out in Division 2.

Item 29 Subsection 6(1)

This item inserts the definition of *credit worthiness*. This definition is, along with the definition of 'consumer credit', central to the purpose of the credit reporting system, which is established to allow credit providers to use certain personal information to determine an individual's 'credit worthiness' and to establish the individual's eligibility for consumer credit. The term 'credit worthiness' is used in the definitions of 'CP derived information' and CRB derived information'. These definitions refer to information that has a bearing on an individual's credit worthiness and is, has or could be used in establishing the individual's eligibility for consumer credit. Accordingly, personal information about the individual in the credit reporting system that is held and maintained by credit reporting bodies in the form of 'credit reporting information' (under Division 2) and credit providers in the form of 'credit eligibility information' (under Division 3) includes information that has a bearing on an individual's credit worthiness and is, has or could be used in establishing the individual's eligibility for consumer credit.

There are three components to the definition of an individual's credit worthiness. These matters are the individual's: eligibility to be provided with consumer credit; history in relation to consumer credit'; or capacity to repay an amount of credit that relates to consumer credit.

Item 30 Subsection 6(1) (definition of *current credit provider*)

This item repeals the definition of *current credit provider*.

This definition is no longer required. The definition of 'consumer credit liability information' includes information about an individual's credit provider in relation to the individual's existing consumer credit liabilities. This means that any credit provider included consumer credit liability information is a current credit provider in relation to an individual.

Item 31 Subsection 6(1)

This item inserts a cross-reference to the definition of *default information* in clause 6Q.

Item 32 Subsection 6(1) (definition of *eligible communications service*)

This item repeals the definition of *eligible communications service*, as this term is no longer used in the credit reporting provisions.

Item 33 Subsection 6(1) (definition of *guarantee*)

This item repeals the existing definition of *guarantee* and replaces it with a new definition that is consistent with the new terms now used in the credit reporting provisions. Specifically, the definition, which provides that a guarantee includes an indemnity given against the default of a person in making a payment in relation to credit, now concludes by making clear that it is a payment in relation to credit that has been applied for by, or provided to, the person for whom the individual is or will be guarantor.

Item 34 Subsection 6(1)

This item inserts the definition of *identification information*. Identification information is a type of information that is included in the definition of 'credit information' (see clause 6N). While the personal information included in this definition does not itself directly refer to an individual's credit obligations, it is necessary to include this personal information in credit information to ensure that the individual can be effectively identified and linked to other personal information about their credit obligations included in their 'credit information'. Credit reporting bodies cannot collect identification information about individuals without collecting or holding other credit information, and can only collect identification information about individuals who are under the age of 18 in certain circumstances (see clause 20C).

The term 'identification information' refers to those types of personal information about an individual that are listed in the definition. No other personal information may be included as identification information in an individual's credit information, and hence in the credit reporting system.

Identification information about an individual means: the individual's full name; any alias or previous name of the individual; the individual's date or birth; and the individual's sex. In addition, the definition includes the individual's current or last known address, and two previous addresses, if any; the name of the individual's current or last known employer; and the individual's driver's licence number (if the individual holds a licence).

The definition does not include any more than two previous addresses for an individual. While there may be circumstances in which an individual may change addresses relatively frequently in a period of time, it is considered that only including the individual's current address and two previous addresses in the individual's identification information sufficiently balances the need to identify the individual accurately with the individual's interests in maintaining the privacy of the individual's previous addresses. This restriction also ensures that there is no possibility of a history of the individual's addresses being compiled.

Item 35 Subsection 6(1)

This item inserts a cross-reference to the definition of *information request* in clause 6R.

Item 36 Subsection 6(1)

This item inserts a cross-reference to the definition of *interested party* in subclauses 20T(3) and 21V(3) (which deal with consultation by a credit reporting body or a credit provider respectively, following an individual's correction request).

Item 37 Subsection 6(1)

This item states that *'licensee'* has the meaning given by the NCCP Act.

Repayment history information can only be disclosed in circumstances where the disclosing credit provider, or the recipient of the information from a credit reporting body, is a licensee. The reason for this is that licensees are subject to responsible lending obligations under the

NCCP Act, and the repayment history information is intended to assist those credit providers in meeting those obligations. Credit providers can only disclose repayment history information to a credit reporting body if the credit provider is a licensee (see paragraph 21D(3)(c)), and can only disclose repayment history information as part of credit eligibility information if the recipient is a licensee (see paragraph 21G(5)(a) – but note that a disclosure to a mortgage insurer is permitted by clause 21L). Credit reporting bodies can only disclose repayment history information to a credit provider that is a licensee (see subclause 20E(4)). Defining the term 'licensee' by referring to its meaning in the NCCP Act ensures that there is a single source for the meaning of the term which assists in identifying a licensee.

Item 38 Subsection 6(1) (definition of *loan*)

This item repeals the definition of *loan* as the term has been replaced by the term 'credit'.

Item 39 Subsection 6(1)

This item inserts the definition of *managing credit*. A credit provider is permitted to disclose credit eligibility information to a person who manages credit provided by the credit provider for use in managing that credit (see subclause 21G(3)). A person who manages credit is included in the definition of an 'affected information recipient' and is subject to the obligations in Division 4, and in particular clause 22E dealing with the use or disclosure of credit eligibility information by credit managers. Agents of credit providers and securitisation entities may also manage credit(see clauses 6H and 6J).

The definition operates by excluding certain matters from the meaning of 'managing credit'. An act relating to the collection of overdue payments in relation to credit is excluded from the meaning of 'managing credit'. The collection of overdue payments is specifically regulated by clause 21M, which provides for disclosures by credit providers of certain limited types of credit eligibility information to debt collectors. It would undermine the protection afforded to credit eligibility information and the operation of clause 21M if a debt collector could also collect credit eligibility information in the guise of managing credit.

In general terms, it is understood that a credit manager is someone who manages credit for a credit provider (but is not an agent of the credit provider), and to whom disclosures are permitted for that purpose. The acts that constitute managing credit are likely to vary depending on the services that a credit manager has agreed to provide to a credit provider. This may vary, for example, from providing all matters relating to the management of credit to only some specific matters. For example, a credit manager may supply a credit provider with customer management or customer assistance services, or may instead supply a variety of data management or back-office services to a credit provider. A credit provider should only disclose credit eligibility information for use by the credit manager where that information is necessary for the credit manager to manage the credit provided by the credit provider. Not all acts that constitute managing credit will require all credit eligibility information to be disclosed to the credit manager, and credit eligibility information shouldn't be disclosed by credit providers to credit managers as a matter of course.

Item 40 Subsection 6(1) (definition of *mortgage credit*)

This item repeals the definition of *mortgage credit* and replaces it with a new definition that is consistent with the new terms now used in the credit reporting provisions. Specifically, the definition now refers to 'consumer credit' as the definition of this term now includes credit for which an individual has made an application, or credit which the individual has been provided, for purposes relating to residential property for investment purposes. The term 'mortgage credit' is used in the definition of 'mortgage insurance purpose' and 'mortgage

insurer' (see items 41 and 42) and is also used in provisions dealing with the collection, use and disclosure of personal information by credit reporting bodies (see Division 2) and credit providers (see Division 3).

Item 41 Subsection 6(1)

This item inserts the definition of *mortgage insurance purpose*.

A credit provider can disclose credit eligibility information to a mortgage insurer for a mortgage insurance purpose (see clause 21L), and a credit reporting body can disclose credit reporting information to a mortgage insurer where the mortgage insurer requests it for a mortgage insurance related purpose (see subclause 20F(1)). This definition is necessary to assist the understanding of a mortgage insurance related purpose. A mortgage insurance purpose is the purpose of assessing: whether to provide insurance to, or the risk of insuring, a credit provider in relation to mortgage credit in certain circumstances; the risk of an individual defaulting on mortgage credit for which the insurer has provided insurance; or the risk of an individual being unable to meet a guarantee provided or proposed to be provided in relation to mortgage credit.

Item 42 Subsection 6(1) (definition of *mortgage insurer*)

This item repeals the definition of *mortgage insurer* and replaces it with a new definition that is consistent with the new terms now used in the credit reporting provisions. A mortgage insurer carries on a business or undertaking that involves providing insurance to credit providers in relation to mortgage credit provided by credit providers to other persons.

In addition, the definition of 'mortgage insurer' now clearly includes a small business operator that meets the requirements of this definition, along with any organisation. This is to ensure effective protection of personal information in the credit reporting system, whether the personal information is held or maintained by a small business operator or an organisation.

Item 43 Subsection 6(1)

This item inserts a cross-reference to the definition of the *National Personal Insolvency Index* in the *Bankruptcy Act* (which has been defined to mean the *Bankruptcy Act 1966*).

Item 44 Subsection 6(1)

This item inserts a cross-reference to the definition of *new arrangement information* in clause 6S.

Item 45 Subsection 6(1)

This item inserts a cross-reference to the definition of *payment information* in clause 6T.

Item 46 Subsection 6(1)

This item inserts a cross-reference to the definition of *penalty unit* in section 4AA of the *Crimes Act 1914* to ensure that the term has the same meaning.

Item 47 Subsection 6(1)

This item inserts the definition of *pending correction request*. The correction procedures set out in Divisions 2 and 3 permit an individual to make a request for the correction of certain personal information to a credit reporting body or a credit provider and for the recipient of the request to make a decision on the correction request, after, if necessary, consulting any other credit reporting body or credit provider. However, credit reporting bodies have obligations to destroy or de-identify credit reporting information after the retention period for the

information has ended (see clause 20V). Destruction or de-identification while a correction request is unresolved would not be appropriate. Accordingly, paragraph 20V(5)(a) deals with the situation where a credit reporting body would otherwise be required to destroy or de-identify information and a correction request is unresolved. It is necessary to have a defined term of 'pending correction request' for this purpose. In addition, clause 20Z imposes certain obligations on credit reporting bodies in relation to dealing with information if there is a pending correction request. As the destruction or de-identification obligations apply to credit reporting bodies, the definition of pending correction request is only focussed on the correction of personal information about an individual that may be held by a credit reporting body – that is, credit information or CRB derived information.

A pending correction request in relation to credit information or CRB derived information is a request made under subclause 20T(1) (which provides that an individual may request the correction of credit reporting information) in relation to which a notice informing the individual of the credit reporting body's decision (to correct the information or not correct the information) has not been given under clause 20U. A pending correction request also means a request made under subclause 21V(1) (which provides that an individual may request the correction of credit eligibility information) where a credit reporting body has been consulted under that clause and in relation to which a notice informing the individual of the credit provider's decision (to correct the information or not correct the information) has not been given under clause 21W.

Item 48 Subsection 6(1)

This item inserts the definition of *pending dispute*. Division 5 contains provisions dealing with complaints by individuals to credit reporting bodies or credit providers about a breach of Part IIIA. Other credit reporting bodies or credit providers must be consulted about a complaint where necessary. In addition, a complaint may be made to a recognised external dispute resolution scheme or to the Commissioner under Part V of the Act. However, credit reporting bodies have obligations to destroy or de-identify credit reporting information after the retention period for the information has ended (see clause 20V). Destruction or de-identification while a dispute is unresolved would not be appropriate. According, paragraph 20V(5)(b) deals with the situation where a credit reporting body would otherwise be required to destroy or de-identify information and a there is an unresolved complaint. It is necessary to have a defined term of 'pending dispute' for this purpose. In addition, clause 20Z imposes certain obligations on credit reporting bodies in relation to dealing with information if there is a pending dispute. As the destruction or de-identification obligations apply to credit reporting bodies, the definition of pending dispute is only focussed on a dispute about an individual's personal information that may be held by a credit reporting body – that is, credit information or CRB derived information.

A pending dispute in relation to credit information or CRB derived information means: a complaint made under clause 23A that relates to the information if a decision about the complaint has not been made under subclause 23B(4); or complaint or other matter relating to the information that is being dealt with by a recognised external dispute resolution scheme; or a complaint made to the Commissioner under Part V.

Item 49 Subsection 6(1)

This item inserts a cross-reference to the definition of *permitted CP disclosure* which has the meaning given to the term by clauses 21J to 21N.

Item 50 Subsection 6(1)

This item inserts a cross-reference to the definition of *permitted CP use* which has the meaning given to the term by clause 21H.

Item 51 Subsection 6(1)

This item inserts a cross-reference to the definition of *permitted CRB disclosure* which has the meaning given to the term by clause 20F.

Item 52 Subsection 6(1)

This item inserts a cross-reference to the definition of *personal insolvency information* which has the meaning given to the term by clause 6U.

Item 53 Subsection 6(1)

This item inserts a cross-reference to the meaning of *pre-screening assessment* which has the meaning given to the term by paragraph 20G(2)(d).

Item 54 Subsection 6(1)

This item inserts the definition of *purchase*. This definition was previously at subsection 6(5D) (and has been repealed by item 66). This term is used in the definitions of 'securitisation arrangement' and 'securitisation related purpose'. The term is defined to clarify that 'purchase' when used in relation to credit, includes the purchase of rights to receive payments relating to the credit. Where the term 'purchase' is used in another context (for example, in subclause 21N(2) in relation to purchasing an interest in a credit provider) this special meaning does not apply.

Item 55 Subsection 6(1)

This item inserts the definition of *regulated information*. An 'affected information recipient' is subject to certain obligations set out in Division 4 in relation to 'regulated information'. The term 'regulated information' is defined by reference to the types of personal information that may be disclosed to affected information recipients under Divisions 2 or 3. Generally, regulated information is 'credit eligibility information' or 'credit reporting information' that has been disclosed to affected information recipients.

An affected information recipient is a term used to refer to certain entities or persons that may be provided with credit reporting information or credit eligibility information in certain circumstances. Where the affected information recipient is a mortgage insurer, a credit reporting body may disclose credit reporting information to a mortgage insurer in certain circumstances (see clause 20F). A credit provider may disclose credit eligibility information to them in certain circumstances (see clause 21L). Where the affected information recipient is a trade insurer, a credit reporting body may disclose credit reporting information to them in certain circumstances (see clause 20F). Where the affected information recipient is a related body corporate, a credit provider may disclose credit eligibility information to them in certain circumstances (see paragraph 21G(3)(b)). Where the affected information recipient is a person who manages credit for a credit provider, a credit provider may disclose credit eligibility information to them in certain circumstances (see paragraph 21G(3)(c)). Where the affected information recipient an entity or adviser of an entity, a credit provider may disclose credit eligibility information to them in certain circumstances (see subclause 21N(2)).

Item 56 Subsection 6(1)

This item inserts a cross-reference to the definition of *repayment history information* which has the meaning given by subclause 6V(1).

Item 57 Subsection 6(1)

This item inserts a cross-reference to the definition of *residential property* in section 204 of the National Credit Code (within the meaning of the National Consumer Credit Protection Act).

Item 58 Subsection 6(1)

This item inserts the definition of *respondent.* This term is used in Division 5 on complaints to identify the credit reporting body or the credit provider to whom the complaint is made under clause 23A.

Item 59 Subsection 6(1)

This item inserts a cross-reference to the definition of *retention period* which has the meaning given by clauses 20W and 20X.

Item 60 Subsection 6(1) (subparagraphs (a)(i) and (ii) of the definition of *securitisation arrangement*)

This item replaces part of the definition of *securitisation arrangement* that previously used the term 'loan' with subparagraphs that use the term 'credit'. The term 'loan' has been repealed because this concept has been replaced with 'credit'.

Item 61 Subsection 6(1) (paragraph (b) of the definition of *securitisation arrangement*)

This item replaces any references to the term 'loans' in the definition of *securitisation arrangement*, with the term 'credit.' The term 'loan' has been repealed because this concept has been replaced with 'credit'.

Item 62 Subsection 6(1)

This item inserts the definition of *securitisation related purpose*. This definition refers to the term 'securitisation arrangement'. Credit reporting bodies may disclose credit reporting information to a credit provider where the provider requires the information for a securitisation related purpose (see subclause 20F(1), and note that the meaning of 'credit provider' for this purpose is modified by subclause 6J(1)). Where the relevant credit reporting information was disclosed to the credit provider for a particular securitisation related purpose, the credit provider can then use the credit eligibility information for that particular purpose (see subclause 21(H)) or disclose credit eligibility information to another credit provider (as defined by subclause 6J(1)) for a securitisation purpose in certain circumstances (see subclause 21J(4)).

A credit provider has a securitisation related purpose in relation to an individual if the purpose is to: assess the risk in purchasing credit provided to, or applied for by, an individual or a person for whom the individual is or may be a guarantor; or to assess the risk in undertaking credit enhancement in relation to credit that is, or may be, purchased or funded by a securitisation arrangement and that has been provided to, or applied for by, the individual or a person for whom the individual is or may be a guarantor.

Item 63 Subsection 6(1) (definition of *serious credit infringement*)

This item repeals the existing definition of *serious credit infringement* and replaces it with a new definition that makes certain changes to the requirements that must be satisfied before an act of an individual will be a serious credit infringement, and also uses terms that are consistent with the new terms now used in the credit reporting provisions. Information about a 'serious credit infringement' can be included in an individual's 'credit information' (see clause 6N) and the term is also used in relation to the collection, use and disclosure of information about a serious credit infringement in by credit reporting bodies (in Division 2) and credit providers (in Division 3).

There are three situations in which the definition of a serious credit infringement can be satisfied. An act of an individual will be a serious credit infringement where the act involves fraudulently obtaining consumer credit, or attempting to fraudulently obtain consumer credit. An act of an individual will also be a serious credit infringement where the act involves fraudulently evading, or attempting to evade, the individual's obligations in relation to consumer credit. Both of these situations involve fraud on the part of the individual.

The third situation in which an act of an individual will be a serious credit infringement includes a number of elements that must be present. The individual must do an act that a reasonable person would consider indicates an intention on the part of the individual to no longer comply with the individual's obligations in relation to consumer credit provided by a credit provider. In addition, the credit provider must take steps that are reasonable in the circumstances to contact the individual about the act, and the credit provider must have been unsuccessful in contacting the individual. The third element is that at least six months must have passed since the provider last had contact with the individual. It is expected that in most cases, where the serious credit infringement relates to an outstanding amount owed by the individual, the earliest date that the period of six months would be calculated from is the date that the outstanding amount was due.

The listing of a serious credit infringement as part of an individual's credit information has significant consequences for the individual's credit worthiness. Where a serious credit infringement is based on fraudulent activity, this activity alone is sufficient to justify listing a serious credit infringement. However, where fraud is not involved, the changes made to the definition which ensure that all reasonable efforts are made to contact the individual and that 6 months has passed since the provider last had contact with the individual recognise that this situation is not as clear-cut as fraud and is instead based on an act that a reasonable person would consider indicates an intention on the part of the individual to no longer comply with the individual's consumer credit obligations.

The requirement for six months to have elapsed since the provider last had contact with the individual before the act can be considered to be a serious credit infringement provides a practical timeframe in which the individual may be able to pay the debt before a serious credit infringement is listed. In some situations, an individual may have moved, for example at the end of a tenancy, with the belief that all outstanding bills have been paid. The individual may not be contactable because the credit provider does not have a forwarding address. The individual may also be willing to pay the outstanding amount and may find out about, and pay, the amount once the credit provider has listed a default in relation to the outstanding amount. Note that the credit provider will be permitted to list a default in relation to the outstanding amount owed by the individual after at least 60 days have elapsed and the other requirements set out in the definition of 'default' are satisfied. In these circumstances, providing an appropriate period of time before the credit provider can list a serious credit infringement will give the individual the opportunity to pay the debt.

It is expected that the registered CR code will provide guidance and direction on relevant matters, such as: how to interpret whether a credit infringement is 'serious' (for example, in determining whether the individual's conduct can be considered fraudulent); how to establish whether reasonable steps have been taken to contact an individual; how to calculate whether at least six months has passed, and what constitutes the last contact with the individual; and whether a serious credit infringement should be listed where there is a dispute between the parties that is not resolved; and the obligations on credit providers to substantiate that a serious credit infringement has occurred. However, the provisions of the registered CR code must be consistent with other provisions in Part IIIA. This means, for example, that where an individual makes a correction request in relation to a serious credit infringement and this request is refused, the credit reporting body or the credit provider will need to provide evidence substantiating the listing. The registered CR code, in dealing with the obligations of credit reporting bodies and credit providers, should deal with the information and evidence that should be provided to substantiate a serious credit infringement.

Item 64 Subsection 6(1)

This item inserts the definition of *trade insurance purpose*.

A credit reporting body can disclose credit reporting information to a trade insurer for a trade insurance purpose where the individual has expressly consented, in writing, to the disclosure of the information to the insurer for the trade insurance purpose (see clause 20F(1)). This definition is necessary to define the trade insurance purpose. A trade insurance purpose is the purpose of assessing: whether to provide insurance to, or the risk of insuring, a credit provider in relation to commercial credit provided by the provider to the individual or another person; or the risk of a person defaulting on commercial credit for which the insurer has provided insurance to the credit provider.

Item 65 Subsection 6(1) (definition of *trade insurer*)

This item repeals the existing definition of *trade insurer* and inserts a new definition that is consistent with the new terms now used in the credit reporting provisions. A trade insurer carries on a business or undertaking that involves providing insurance to credit providers in relation to commercial credit provided by credit providers to other persons.

In addition, the definition of 'trade insurer' now clearly includes a small business operator that meets the requirements of this definition, along with any organisation. This is to ensure effective protection of personal information in the credit reporting system, whether the personal information is held or maintained by a small business operator or an organisation.

Item 66 Subsections 6(5A) to (5D)

This item repeals subsections 6(5A), (5B) and (5C) as they have been replaced by the definition of credit reporting business set out in clause 6P.

This item also repeals subsection 6(5D), which refers to the meaning of purchase of a loan. Item 54 inserts a definition of 'purchase' in subsection 6(1) based on the definition in subsection 6(5D).

Item 67 Subsection 6(10)

Subsection 6(10) sets out the definition of family as used in the definition of *credit*. This item replaces the term 'credit' with the term 'consumer credit' in that definition as the definitions have been restructured and the term 'family' is now used in the definition of 'consumer credit' rather than in the definition of 'credit'.

Item 68 At the end of subsection 6D(4)

This item inserts a new paragraph at the end of subsection 6D(4) which refers to a 'credit reporting body'. This means that a credit reporting body that is a small business operator will be treated as an organisation for the purposes of the Act.

The definition of 'organisation' in section 6C excludes a small business operator. However, subsection 6D(4) specifies certain entities that are not small business operators and hence which are treated as organisations. This amendment adds an additional paragraph to section 6D(4) referring to a credit reporting body. This means that a credit reporting body that is a small business is not, for the purposes of the Act, a small business operator. It is appropriate that small business operators are permitted to be credit reporting bodies and play a role in the credit reporting system. However, those small business operators should be subject to the obligations in the Act that apply to other organisations, such as the APPs, and the obligations in the Act that apply to credit reporting bodies, in particular, the obligations set out in Part IIIA of the Act.

Item 69 After section 6F

This item inserts a new Division containing key definitions relating to credit reporting.

Division 2 – Key definitions relating to credit reporting

Subdivision A – Credit provider

This Subdivision deals with the definitions of the term 'credit provider'. Clause 6G sets out the general definition of 'credit provider'. Clauses 6H, 6J and 6K deal with specific situations in which an organisation or small business operator will also be considered to be a 'credit provider' for the purposes set out in those clauses.

Clause 6G Meaning of *credit provider*

This provision inserts the meaning of *credit provider*. The general meaning of 'credit provider', certain additional situations which extend the general meaning of 'credit provider', and certain exclusions to the meaning of 'credit provider' are dealt with in this provision.

Subclause (1) sets out the general definition of 'credit provider'. Paragraph (a) states that a 'bank' is a credit provider, and 'bank' is defined in section 6(1). Paragraph (b) states that an organisation or small business operator that carries on a business or undertaking of which a substantial part of that business or undertaking is the provision of credit will be a credit provider. In this context, substantial connotes both value and proportion. An organisation or small business operator could satisfy this aspect of the definition where its activities relating to the provision of credit involved substantial amounts of money, even if its lending activities did not constitute the dominant part of the corporation's overall business. However, in order to be a substantial part of the entity's business, the loans provided by a corporation would have to be an essential or important part of its business, and not merely incidental to it.

Paragraph (c) deals with organisations or small business operators that issue credit cards. Paragraph (c) provides that an organisation or small business operator that carries on a retail business and which, in the course of the business, issues credit cards to individuals in connection with the sale of goods, or the supply of services, by the organisation or small business operator will be a credit provider.

Paragraph (1)(d) provides that regulations may prescribe an agency, organisation or small business operator that carries on a business or undertaking that involves providing credit is a credit provider for the purposes of clause 6G. This provision provides the option of dealing with situations where an agency, organisation or small business is involved in providing

credit, but does not satisfy the requirements of paragraph (1)(b). It is expected that regulations will be made to prescribe Indigenous Business Australia as a credit provider.

Subclause (1) makes clear that small business operators are, if they satisfy the requirements of the provision (in the case of paragraph (d), this includes being prescribed by regulations), credit providers that are subject to the credit reporting provisions. However, a credit provider that is a small business operator may not be an APP entity subject to the APPs depending on the nature of their business and the operation of the small business exemption in section 6D and related provisions. This is different to the position for small business operators that are credit reporting bodies, which are subject to both the credit reporting provisions and the Act as a whole (including the APPs) because they are excluded from the definition of a 'small business operator' (see item 68).

Subclauses (2), (3) and (4) deal with other situations in which an organisation or small business operator may be a credit provider. However, the organisation or small business operator will be a credit provider only in relation to the circumstances set out in these provisions. This means that the organisation or small business operator is a credit provider only for limited situations, and not for their whole business or undertaking. These situations only apply if the organisation or small business operator is not a credit provider under subclause (1).

Subclause (2) deals with situations in which an organisation or small business operator (known in this provision as the 'supplier') provides credit in relation to the sale of goods or the supply of services. If the supplier permits the repayment, whether in full or in part, of the amount of credit to be deferred for at least 7 days, and the supplier is not already a credit provider under subclause (1), then the supplier will be a credit provider, but only in relation to the credit which satisfies this provision.

Subclause (3) deals with situations in which an organisation or small business operator (known in this provision as the 'lessor') provides credit in connection with the hiring, leasing or renting of goods. If the lessor provides such credit and the credit is in force for at least 7 days, and no amount, or an amount that is less than the value of the goods, is paid as a deposit for the return of the goods, and the lessor is not already a credit provider under subclause (1), then the lessor will be a credit provider, but only in relation to the credit which satisfies this provision.

Subclause (4) provides that an organisation or small business operator that satisfies the requirements of clauses 6H, 6H and 6K is a credit provider.

Subclauses (5) and (6) set out situations in which an organisation or small business operator are excluded from the meaning of credit provider, even if they may satisfy any of the other provisions in clause 6G. Subclause (5) makes clear that any organisation or small business operator that acts in the capacity of a real estate agent, a general insurer (within the meaning of the *Insurance Act 1973*), or an employer of an individual is not a credit provider while acting in that capacity. It is not consistent with the objectives of the credit reporting system to permit personal information in the credit reporting system to be disclosed or used for any purpose of a real estate agent, a general insurer, or an employer of an individual. In particular, personal information in the credit reporting system must not be used in relation to the management of rental properties, and this prohibition includes any use for assessing potential tenants for rental properties. To the extent that any other organisation or small business operator that would otherwise be a credit provider under clause 6G performs the functions of a real estate agent, including the assessment of potential tenants for rental properties, that organisation or small business operator would not be a credit provider for that

purpose. Collection, use or disclosure by a credit reporting body or a credit provider for that purpose would be a breach of the credit reporting provisions and may, depending on the circumstances, be a credit reporting offence. Similarly, an organisation or small business operator that was acting in its capacity as an employer of an individual would not be a credit provider for any employment related purpose (including, for example, assessing an applicant for a position in which the organisation or small business operator would be the individual's employer).

Subclause (6) provides that regulations may specify that an organisation or small business operator is not a credit provider if it is included in a class of organisations or small business operators prescribed by the regulations. The regulations will operate to ensure that an organisation or small business operator is not a credit provider despite the operation of subclauses (1) to (4), under which the organisation or small business operator would otherwise have been a credit provider.

Clause 6H Agents of credit providers

This provision sets out the circumstances in which an organisation or small business operator that is acting as the agent of a credit provider will be considered to be a credit provider while acting as the credit provider's agent.

Subclause (1) provides that an organisation or small business operator will be acting as an agent of a credit provider (the principal) if it is performing, on the principal's behalf, a task that is reasonably necessary in processing an application for credit made to the principal, or a task that is reasonably necessary in 'managing credit' provided by the principal.

Subclause (2) limits the application of subclause (1). If an organisation or small business operator is taken to be a credit provider because it is already acting as the agent of another credit provider (the principal), then any organisation or small business operator that performs tasks for that agent does not become a credit provider under the operation of subclause (1). Essentially, this provision prevents the agent of an agent becoming the agent of the principal credit provider for the purposes of the credit reporting provisions.

Subclauses (3) and (4) state the effect of the agent satisfying the requirements to be a credit provider under subclause (1). Subclause (3) provides that, where subclause (1) applies in relation to credit provided by the principal, the credit is taken for the purposes of the Act to have been provided by both the principal and the agent. Subclause (4) provides that, where subclause (1) applies in relation to an application for credit made to the principal, the application for credit is taken for the purposes of the Act to have been made to both the principal and the agent.

This provision makes clear that small business operators are, if they satisfy the requirements of the provision, credit providers for the purpose of this provision that are subject to the credit reporting provisions. However, a credit provider that is a small business operator may not be an APP entity subject to the APPs depending on the nature of their business and the operation of the small business exemption in section 6D and related provisions. This is different to the position for small business operators that are credit reporting bodies, which are subject to both the credit reporting provisions and the Act as a whole (including the APPs) because they are excluded from the definition of a 'small business operator' (see item 68).

Clause 6J Securitisation arrangements etc.

This provision provides the circumstances in which an organisation or small business operator that is a securitisation entity will be considered to be a credit provider.

Subclause (1) sets out the circumstances in which an organisation or small business operator that is a securitisation entity will be a credit provider. An organisation or small business operator that is a securitisation entity must carry on a business that is involved in either or both of: a 'securitisation arrangement'; or managing credit that is the subject of a securitisation arrangement. The securitisation entity must also perform a task that is reasonably necessary for either purchasing, funding or managing, or processing an application for, credit by means of a securitisation arrangement, or reasonably necessary for undertaking 'credit enhancement' in relation to credit. In addition, the credit referred to must have been provided by, or be the subject of an application to, the original credit provider. In these circumstances, the securitisation entity will be a credit provider while it performs any such task set out above.

Subclause (2) limits the application of subclause (1). If an organisation or small business operator is taken to be a credit provider because it is already acting as a securitisation entity of another credit provider (the original credit provider), then any organisation or small business operator that performs tasks for the securitisation entity does not become a credit provider under the operation of subclause (1).

Subclauses (3) and (4) state the effect of the securitisation entity satisfying the requirements to be a credit provider under subclause (1). Subclause (3) provides that, where subclause (1) applies in relation to credit provided by the original credit provider, the credit is taken for the purposes of the Act to have been provided by both the principal and the securitisation entity. Subclause (4) provides that, where subclause (1) applies in relation to an application for credit made to the original credit provider, the application for credit is taken for the purposes of the Act to have been made to both the principal and the securitisation entity.

This provision makes clear that small business operators are, if they satisfy the requirements of the provision, credit providers for the purpose of this provision that are subject to the credit reporting provisions. However, a credit provider that is a small business operator may not be an APP entity subject to the APPs depending on the nature of their business and the operation of the small business exemption in section 6D and related provisions. This is different to the position for small business operators that are credit reporting bodies, which are subject to both the credit reporting provisions and the Act as a whole (including the APPs) because they are excluded from the definition of a 'small business operator' (see item 68).

Clause 6K Acquisition of the rights of a credit provider

This provision provides that an organisation or small business operator which acquires the rights of a credit provider in relation to the amount of credit will be considered to be a credit provider in relation to that particular amount of credit.

Subclause (1) sets out the circumstances in which an organisation or small business operator that acquires the rights of a credit provider will be taken to be a credit provider. Where the organisation or small business operator (known as the acquirer) acquires (whether by assignment, subrogation or any other means) the rights of the original credit provider in relation to the repayment of an amount of credit, then the acquirer will (subject to paragraph (b)) be a credit provider only in relation to that credit.

Paragraph (1)(b) limits the application of paragraph (1)(a). If an organisation or small business operator that is an acquirer is already a credit provider under subclause 6G(1), then the acquirer is not also a credit provider under subclause (1).

Subclauses (2) and (3) state the effect of the acquirer satisfying the requirements to be a credit provider under subclause (1). Subclause (2) provides that, where subclause (1) applies in relation to credit provided by the original credit provider, the credit is taken for the

purposes of the Act to have been provided by both the original credit provider and the acquirer. Subclause (3) provides that, where subclause (1) applies in relation to an application for credit made to the original credit provider, the application for credit is taken for the purposes of the Act to have been made to both the original credit provider and the acquirer.

This provision makes clear that small business operators are, if they satisfy the requirements of the provision, credit providers for the purpose of this provision that are subject to the credit reporting provisions. However, a credit provider that is a small business operator may not be an APP entity subject to the APPs depending on the nature of their business and the operation of the small business exemption in section 6D and related provisions. This is different to the position for small business operators that are credit reporting bodies, which are subject to both the credit reporting provisions and the Act as a whole (including the APPs) because they are excluded from the definition of a 'small business operator' (see item 68).

Subdivision B – Other definitions

This Subdivision sets out other key credit reporting definitions.

Clause 6L Meaning of *access seeker*

This provision inserts the meaning of *access seeker*. The term 'access seeker' is used to describe a person who requests access to credit reporting information from a credit reporting body (see clause 20R) or credit eligibility information from a credit provider (see clause 21T), and is also used in the offence provisions in Division 6.

Subclause (1) provides that an access seeker in relation to credit reporting information or credit eligibility information about an individual is either the individual, or a person who is assisting the individual to deal with a credit reporting body or credit provider. Where it is a person assisting the individual, the person must be authorised, in writing, by the individual to make the access request in relation to the individual's information.

Subclause (2) provides certain exceptions to subclause (1). An individual is not permitted to authorise a person under subclause (1) if the person is a credit provider, a mortgage insurer, a trade insurer, or a person who is prevented from being a credit provider by subclause 6G(5) or (6). The access provisions should not be used by these persons because any access would circumvent the provisions prescribing the circumstances in which these entities or persons can collect, or are prohibited from collecting, credit reporting information or credit eligibility information about the individual. Subclauses 6G(5) and (6) prohibit a real estate agent, a general insurer, or an employer from being a credit provider, or any organisation or small business entity that is prescribed by regulations from being a credit provider. A person who is any of these cannot be authorised as an access seeker for an individual.

Subclause (3) provides that the National Relay Service is excluded from the definition of 'access seeker'. The National Relay Service provides assistance to individuals to communicate with others. If the National Relay Service is assisting an individual to deal with a credit reporting body or credit provider they would fall within subclause (1) and be required to be authorised in writing by the individual. However, because of the way the National Relay Service operates, the need for an individual to give written authorisation may be problematic in some situations. In these circumstances it would not be appropriate to impose an obligation on an individual to authorise the National Relay Service in writing before seeking the Service's assistance to communicate with a credit reporting body or credit provider.

Clause 6M Meaning of *credit* and *amount of credit*

This provision inserts the meaning of *credit* and *amount of credit*. The term 'credit' is central to the credit reporting system and replaces the previous term 'loan'. The term 'amount of credit' is used in the definitions of 'consumer credit liability information' (see item 10), 'credit worthiness' (see item 29), 'credit provider' (see clause 6G) and 'new arrangement information' (see clause 6S).

Subclause (1) states that 'credit' is a contract, arrangement or understanding under which: payment of a debt owed by one person to another person is deferred; or one person incurs a debt to another person and defers the payment of the debt. In the absence of a written agreement allowing deferral of the payment, the provision of credit requires a mutual understanding between the individual and the relevant entity that a credit contract, arrangement or understanding has been entered into, and the terms of that contract, arrangement or understanding. It may not be sufficient that the individual has not paid the debt, and the entity has failed to enforce payment of it. Whether an entity has provided credit is a question of fact, and an assessment would need to be made on a case by case basis.

Subclause (3) provides certain examples of what satisfies the meaning of 'credit', without limiting the definition set out in subclause (1).

Subclause (2) states that the term 'amount of credit' refers to the amount of the debt that is actually deferred, or may be deferred, but does not include any fees or charges payable in connection with the deferral of the debt.

Clause 6N Meaning of *credit information*

This provision inserts the meaning of *credit information*. 'Credit information' is disclosed by credit providers (see clause 21D) and collected by credit reporting bodies (see clauses 20C and 20D).

Credit information is the basic category of personal information in the credit reporting system. The term credit information comprises a defined list of certain kinds of personal information that are relevant to the purpose of the credit reporting system. However, any information that would fall within the definition of sensitive information in section 6(1) of the Act is expressly excluded from credit information.

The following types of personal information included in the definition of credit information are separately defined in section 6(1): 'consumer credit liability information' (see item 10 - this type of information includes four of the five new types of personal information that are permitted as part of the move to more comprehensive credit reporting); 'court proceedings information' (see item 12); and 'identification information' (see item 34). The following types of personal information are separately defined in Division 2, which sets out key definitions relating to credit reporting: 'default information' (see clause 6Q); 'information requests' (see clause 6R); 'new arrangement information' (see clause 6S); 'payment information' (see clause 6T); 'personal insolvency information' (see clause 6U) and 'repayment history information' (see clause 6V - this type of information is the fifth type of personal information that is permitted as part of the move to more comprehensive credit reporting).

The definition of credit information includes, at paragraph (e), information about the type and amount of consumer or commercial credit sought in an application made by an individual to a credit provider (further description of what 'type' and 'amount' mean is given in relation to item 10).

In addition, credit information includes two other kinds of personal information: information about certain publicly available information about the individual that relates to the

individual's activities in Australia or the external Territories and their credit worthiness; and information that is the opinion of a credit provider that the individual has committed a' serious credit infringement' (defined in section 6(1), see item 63).

The type of publicly available information that can be included in an individual's credit information is limited by paragraph (k). The publicly available information about the individual must relate to the individual's activities in Australia or the external Territories and the individual's credit worthiness. This limitation ensures that information about an individual's foreign activities is not included. In addition, the information must relate to the individual's credit worthiness. This is consistent with the purpose of the credit reporting system. The other restriction set out in paragraph (k) is that the information must not be court proceedings information about the individual or information that is entered on the National Personal Insolvency Index. Both of these types of information are publicly available, but the inclusion of these types of information about an individual are specifically dealt with by paragraphs (i) and (j), and separately defined in section 6(1) and clause 6U respectively.

It is expected that the registered CR code will provide further explanation of the meaning of 'publicly available information' to assist in understanding this term and the types of information to which it applies. Whether information is publically available information is a decision that must be made on a case-by-case basis, taking into account all relevant circumstances, such as the extent to which access to the information is restricted in some way, for example by a fee.

Clause 6P Meaning of *credit reporting business*

This provision inserts the meaning of *credit reporting business*. The term 'credit reporting business' is used in the definition of a 'credit reporting body' (see item 26).

Subclause (1) provides that a 'credit reporting business' is a business or undertaking that involves collecting, holding, using or disclosing personal information about individuals for the purpose of, or for purposes including the purpose of, providing an entity with information about the credit worthiness of an individual. Subclause (2) makes clear that subclause (1) applies whether or not the information is provided for profit or reward, or provided, or intended to be provided, for the purposes of assessing an application for consumer credit.

Subclause (3) sets out an exception to subclause (1) where a credit provider provides information about the credit worthiness of an individual to a related body corporate (in addition, see paragraph 21G(3)(b), which permits the disclosure of credit eligibility information to a related body corporate).

Division 3 sets out 'permitted CP disclosures' under which a credit provider is permitted to disclose credit eligibility information, including, for example, to other credit providers with the consent of the individual (see subclause 21J(1)). A credit provider that makes a 'permitted CP disclosure' would not, as a result of making that specific permitted disclosure, fall within the general definition set out in subclause (1).

Subclause (4) provides that regulations may exclude certain businesses or undertakings from the definition of a credit reporting business. A business or undertaking is not a credit reporting business if it is included in a class of businesses or undertakings prescribed by the regulations.

The definition of a 'credit reporting business' does not contain a dominant purpose test, which previously featured in the former definition of this term that has been repealed (see item 27). Any business or undertaking that falls within the terms of subclause (1) is regarded as a credit reporting business. This does not require, for example, a consideration of whether

the activities of a credit reporting business are a large or small component of the overall activities of the business or undertaking. If the activities of the business or undertaking involve collecting, holding, using or disclosing personal information about individuals, either wholly or partly for the purpose of providing an entity with information about an individual's credit worthiness, then the business or undertaking is a credit reporting business. It is considered appropriate that any business or undertaking that is performing these activities should be subject to the obligations set out in the credit reporting provisions. To the extent that the business or undertaking does other activities that are not part of its credit reporting business, the business or undertaking will be subject to the APPs. In addition, a credit reporting body that is a small business operator is excluded from the definition of a small business operator and so will be subject to the APPs (see item 26).

Clause 6Q Meaning of *default information*

This provision inserts the meaning of *default information* in relation to consumer credit defaults and guarantor defaults. 'Default information' is a type of information that can be included in an individual's 'credit information' (see clause 6N). The term is also used in the definitions of 'new arrangement information' (see clause 6S) and 'payment information' (see clause 6T). A credit provider can, subject to certain requirements, disclose 'default information' as part of 'credit information' to a credit reporting body (see paragraph 21D(3)(d)), and must disclose 'payment information' in relation to default information it has disclosed to a credit reporting body (see clause 21E). A credit provider can also disclose certain default information to a debt collector (see subclause 21M(2)).

Default information that is included in an individual's 'credit information' can only be about 'consumer credit', whether the individual is the borrower or the guarantor.

Subclause (1) deals with defaults by an individual that has been provided with consumer credit by a credit provider (that is, a borrower). Default information about an individual is information about a payment (which includes a payment that is wholly or partly a payment of interest) that the individual is overdue in making in relation to consumer credit provided to the individual by the credit provider. In addition, the individual must be at least 60 days overdue in making the payment, and the provider must have given the individual a written notice informing the individual of the overdue payment and requesting the individual pay the amount of the overdue payment. However, the overdue payment cannot be default information if the provider is prevented by a statute of limitations from recovering the amount of the overdue payment. In addition, the overdue payment must be for an amount that is equal to or more than $100, or such other higher amount that is prescribed by regulations. This amount is based on balancing the need for credit providers to assess adequately the credit risk of an individual against the disproportionate consequences of listing less significant debts. It is necessary for regulations to be able to prescribe a higher amount in order for it to be changed from time to time based on changing circumstances.

Subclause (2) deals with defaults by an individual that is a guarantor in relation to consumer credit provided to another individual by a credit provider. Default information about an individual that is a guarantor is information about a payment that the individual is overdue in making as a guarantor in relation to a guarantee given against any default by the borrower in repaying all or any of the deft deferred under consumer credit provided by the provider to the borrower. In addition, the provider must have given the individual written notice of the borrower's default that gave rise to the obligation of the guarantor to make the overdue payment, and the written notice must request that the individual pay the amount of the overdue payment. At least 60 days must have passed since the day on which the notice was given and the provider must have taken other steps (in addition to giving the notice to the

guarantor) to recover the amount of the overdue payment from the guarantor). The provider must also not be prevented by a statute of limitations from recovering the amount of the overdue payment from the guarantor.

If the amount of the overdue payment is less than $100, or any such higher amount prescribed by the regulations, the credit provider is not able to include default information about that overdue amount in the guarantor's 'credit information' An overdue payment of less than $100 or the prescribed amount is not a default due to the operation of paragraph (1)(d). Subclause (2) only operates where the guarantee relates to a default of the borrower.

Clause 6Q clearly excludes statute barred debts from the definition of default information. This means that where the credit provider is prevented by a statute of limitations from recovering the amount of the overdue payment from the individual, the credit provider cannot have that overdue payment included as default information in the individual's 'credit information'. Similarly, a credit provider is prohibited from including default information in an individual's 'credit information' where the individual was a guarantor against the default of another person and the credit provider is prevented from a statute of limitations from recovering the amount of the overdue payment from the guarantor.

It is expected that the registered CR code will provide guidance around the operation of the definition, for example on such matters as the timeframes for giving written notice to individuals.

Clause 6R Meaning of *information request*

This provision inserts the meaning of *information request*. An 'information request' can be included in an individual's 'credit information' (see clause 6N) and refers to a request for information about an individual made to a credit reporting body. A credit reporting body can disclose credit reporting information to a credit provider, mortgage insurer or trade insurer in response to a request for information (see clause 20F). A credit reporting body may retain an information request about an individual for a specified period (see clause 20W).

The meaning of 'information request' varies depending on whether the request for information is made by a credit provider, mortgage insurer, or trade insurer. These differences reflect the circumstances in which a credit reporting body is permitted to disclose credit reporting information to these entities.

Subclause (1) deals with an information request by a credit provider. An information request refers to the circumstances when a credit provider has sought information about an individual from a credit reporting body in connection with an application for 'consumer credit' or 'commercial credit', or for a 'credit guarantee purpose' of the provider, or for a 'securitisation related purpose' of the provider.

Subclause (2) deals with an information request by a mortgage insurer. An information request refers the circumstances when a mortgage insurer has sought information about an individual from a credit reporting body in connection with the provision of insurance to a provider in relation to 'mortgage credit' provided to the individual or a person for whom the individual is, or proposes to be, a guarantor.

Subclause (3) deals with an information request by a trade insurer. An information request refers to the circumstances where a trade insurer has sought information about an individual that from a credit reporting body in connection with the provision of insurance to a provider in relation to 'commercial credit' provided to the individual or another person.

Clause 6S Meaning of *new arrangement information*

This provision inserts the meaning of *new arrangement information* in relation to consumer credit defaults and serious credit infringements. 'New arrangement information' can be included in an individual's 'credit information' (see clause 6N). A credit provider can disclose 'new arrangement information' to a credit reporting body as 'credit information' (see clause 21D). 'New arrangement information' about an individual that is held or maintained by a credit reporting body is subject to specific retention periods (see clause 20W).

Where an individual is overdue in making payments in relation to consumer credit a credit provider may choose to enter into a new arrangement with the individual. Such a new arrangement only satisfies the definition of 'new arrangement information' if the credit provider has previously disclosed 'default information' or a 'serious credit infringement' in relation to the individual's overdue payments. The new arrangement may either vary the original consumer credit arrangements or provide the individual with new consumer credit (either by the original credit provider or a different credit provider) that relates, in whole or in part, to the previous consumer credit. In some circumstances prior to a default, the credit provider and the individual may agree on a hardship arrangement, as provided for in the NCCP Act. Hardship arrangements that satisfy the requirements of the NCCP Act are not included within the meaning of 'new arrangement information'. Similarly, any new arrangement made in relation to consumer credit where the credit provider has not disclosed default information or a serious credit infringement in relation to that consumer credit is not included in the meaning of 'new arrangement information'. It is considered that any such arrangements may appear to be too similar to hardship arrangements to effectively distinguish between them, and increase the risk that individuals may not seek hardship arrangements as permitted in appropriate circumstances.

Once new arrangement information has been included in an individual's credit information, the consumer credit to which that new arrangement relates is treated in the same way as any other consumer credit. This means that if, for example, the individual defaults on the consumer credit provided as a result of the new arrangement, that default can be disclosed as part of the individual's credit information. Where the new arrangement has the effect of rendering the individual no longer overdue in respect of their payments then the credit provider must disclose the relevant 'payment information' in relation to the previously reported default to the credit reporting body. The question of whether the arrangement has the effect of rendering the individual no longer overdue will depend on the intention of the parties as indicated by the terms of the arrangement and any other circumstances. It is expected that the registered CR code will provide further guidance on when the new arrangement has the effect of rendering the individual no longer overdue in respect of their payments.

Subclause (1) deals with 'new arrangement information' where a credit provider has previously disclosed to a credit reporting body 'default information' about an individual that relates to a payment the individual is overdue in making in relation to consumer credit. Where, as a result of this occurring, the provider has varied the terms and conditions of the original consumer credit, or the provider or a different credit provider has provided the individual with new consumer credit that relates, wholly or in part, to the original amount of credit, then a statement that this has occurred is new arrangement information. Such as statement can then be included in the individual's 'credit information'. An arrangement would normally involve a significant variation of the main elements of the contract such as the period of the loan, or the size and frequency of repayments. On this basis, an arrangement would not include, for example, a verbal agreement to allow a one-off later

payment. It is expected that the registered CR code will provide further guidance on what new arrangement fall within paragraph 6S(1)(c) for the purposes of this provision.

Subclause (2) deals with 'new arrangement information' where a credit provider has previously disclosed to a credit reporting body the provider's opinion that the individual has committed a 'serious credit infringement' in relation to consumer credit provided by the provider. Where, as a result of the provider having that opinion, the provider has varied the terms and conditions of the original consumer credit, or the provider or a different credit provider has provided the individual with new consumer credit that relates, wholly or in part, to the original amount of credit, then a statement that this has occurred is new arrangement information. Such as statement can then be included in the individual's 'credit information'.

Clause 6T Meaning of *payment information*

This provision inserts the meaning of *payment information*. 'Payment information' can be included in an individual's 'credit information' (see clause 6N). Where a credit provider has disclosed 'default information' about an individual to a credit reporting body, then the credit provider must disclose 'payment information' that satisfies the terms of this definition to the credit reporting body (see clause 21E). A credit provider is prohibited from disclosing 'default information' to a debt collector if the credit provider holds 'payment information' (see clause 21M). 'Payment information' about an individual that is held or maintained by a credit reporting body is subject to specific retention periods (see clause 20W).

Payment information about an individual is a statement that the amount of an overdue payment has been paid, specifying the day the payment was made. Payment information must relate to default information that a credit provider has disclosed about the individual to a credit reporting body, and must refer to the payment of the amount of the overdue payment, where the payment is made on any day after the default information has been disclosed.

A partial payment of an overdue payment is not 'payment information'. When the overdue payment is wholly paid (whether by a single payment or a series of payments) then the 'payment information' must be disclosed. It is expected that the registered CR code will provide guidance on payment information, such as how the accrual of fees on an overdue payment is to be treated.

Clause 6U Meaning of *personal insolvency information*

This provision inserts the meaning of *personal insolvency information*. 'Personal insolvency information' can be included in an individual's 'credit information' (see clause 6N) and may be collected by a credit reporting body (consistent with the requirements set out in clause 20C). 'Personal insolvency information' about an individual that is held or maintained by a credit reporting body is subject to specific retention periods for different types of information included in the definition of 'personal insolvency information' (see clause 20X). Disclosure by a credit provider of 'personal insolvency information' to a debt collector is subject to specific conditions (see clause 21M).

Paragraph (1)(a) provides that 'personal insolvency information' about an individual must be information that is entered or recorded in the National Personal Insolvency Index. The Index is an official source of personal insolvency information and also sets out the different categories of personal insolvency permitted by the Bankruptcy Act. Paragraph (1)(b) sets out the types of personal insolvency information on the Index which are included in the definition of 'personal insolvency information'.

Subclause (2) provides that information which relates to certain matters is excluded from the meaning of 'personal insolvency information'.

Only the specified types of information on the National Personal Insolvency Index set out in paragraph (b) (and subject to the exclusions in subclause (2)) are permitted to be included as 'personal insolvency information' for the purposes of an individual's 'credit information'. Any other personal information about an individual on the National Personal Insolvency Index cannot be collected as 'credit information'. By providing specifically in paragraph (b) for the personal information on the National Personal Insolvency Index that can be included in personal insolvency information, it is understood that any other information on the Index that is not included in paragraph (b) could not be collected as publicly available information.

Subclause (3) recognises that the Bankruptcy Act sets out the meaning of certain terms and ensures any terms used in paragraphs (1)(b) or (2)(a) have the same meaning as they do in the Bankruptcy Act.

Clause 6V Meaning of *repayment history information*

This provision inserts the meaning of *repayment history information*. 'Repayment history information' can be included in an individual's 'credit information' (see clause 6N). The circumstances in which a credit reporting body can collect or disclose 'repayment history information' are restricted (see clauses 20C and 20E respectively) and the circumstances in which this type of information can be disclosed by a credit provider are also restricted (see clauses 21D and 21G). 'Repayment history information' about an individual that is held or maintained by a credit reporting body is subject to a specific retention period (see clause 20W).

Repayment history information is one of the five types of credit information that are permitted to be included in the credit reporting system as part of the move towards a more comprehensive credit reporting system. The other four types of information that are permitted to be included in the credit reporting system as part of the move to a more comprehensive credit reporting are included in the definition of 'consumer credit liability information' (see item 10).

Application, transitional and savings provisions are set out in schedule 6 of the Bill. Part 3 of schedule 6 deals with the application of the credit reporting provisions. Item 4(6) provides that the definition of 'repayment history information' commences on Royal Assent of the Bill. This means that, on commencement of the Bill, repayment history information that is collected and disclosed can relate to repayment history from the period between Royal Assent and commencement. As clause 2 of the Bill provides that the credit reporting provisions commence 9 months after Royal Assent, this means that 9 months of repayment history information may be collected or disclosed on commencement. This is subject to the obligations set out in clause 6V and the credit reporting provisions, as well as any obligations set out in the regulations made pursuant to subclause (2) or contained in the registered CR code.

Subclause (1) provides that repayment history information about consumer credit provided to an individual is information about whether or not the individual has met an obligation to make a monthly payment that is due and payable in relation to the consumer credit. The information may also include the day on which the monthly payment is due and payable and, if the payment is made after the day on which the payment was due, the day on which the individual makes the payment.

Subclause (2) provides that the regulations may make provision in relation to: whether or not an individual has met an obligation to make a monthly payment; and whether or not a payment is a monthly payment. It is anticipated that regulations will be made to deal with these matters. In addition, it is expected that the registered CR code will provide further

guidance and set out further requirements in relation to the elements of repayment history information, including the calculation of monthly payments and other related matters. This is expected to include requirements and guidance dealing with how repayment history that is subject to other periods of repayment (whether weekly, fortnightly, or some other period of time) will be listed on a monthly basis. In addition, the registered CR code may deal with matters such as grace periods before listing repayment history information and any other relevant matters.

Division 3 – Other matters

Item 70 Paragraphs 7(1)(a) and 8(1)(a)

These paragraphs deal with certain acts and practices. This item replaces the term 'credit reporting agency' with the term 'credit reporting body' as this is the term that is now being used.

Item 71 Sections 11A and 11B

This item repeals sections 11A and 11B as the definitions of credit reporting agencies and credit providers set out in these sections have now been replaced.

Item 72 Part IIIA

This provision repeals Part IIIA and substitutes a new Part IIIA on credit reporting.

Division 1 - Introduction

Clause 19 Guide to this Part

This provision is a guide to the Part.

Division 2 – Credit Reporting Bodies

Subdivision A – Introduction and application of this Division etc.

Clause 20 Guide to this Division

This provision is a guide to the Division.

Clause 20A Application of this Division and the Australian Privacy Principles to credit reporting bodies

This provision states that the Division only applies to credit reporting bodies in relation to their handling of credit reporting information; CP derived information; de-identified information; and pre-screening assessments.

This provision defines the approach taken to the regulation of credit reporting bodies. This Division provides a complete set of rules that apply to credit reporting bodies in relation to these categories of information. As the APPs don't apply to those categories of information it is necessary to ensure that the rules for credit reporting bodies deal with all relevant matters that would otherwise be covered by the APPs.

Credit reporting bodies have obligations in relation to these four categories of information. Most of the provisions in this Division relate to the handling of credit reporting information, which is defined to include both credit information and CRB derived information. Specific provisions relate to pre-screening assessments (clauses 20H and 20J) and credit reporting information that has been de-identified (clause 20M). While a credit reporting body may not hold CP derived information, clause 20T imposes obligations on credit reporting bodies to provide assistance to an individual who wishes to correct credit information, CRB derived information, or CP derived information about the individual. If the credit reporting body

holds at least one of these categories of information they have certain correction obligations, and the ability to consult with another credit reporting body or credit provider as required.

The requirements set out in this Division apply to these categories of information instead of the APPs – that is, the APPs do not apply and are replaced by these requirements. The APPs do not generally apply to de-identified information, which is why this category of information is not included in subclause (2). The reasons for regulating credit reporting information that has been de-identified are set out in the discussion of clause 20M.

To the extent that a credit reporting body handles any other personal information, the handling of that personal information will be regulated by the Australian Privacy Principles.

Subdivision B – Consideration of information privacy

Clause 20B Open and transparent management of credit reporting information

This provision is based on the obligations set out in APP 1, modified to apply specifically to credit reporting bodies and their handling of credit reporting information.

Subclause (1) states the object of the provision.

Subclause (2) imposes a general requirement on credit reporting bodies to take reasonable steps to implement practices, procedures and systems in relation to their credit reporting business that will ensure compliance with the requirements of the Division and the registered CR code and to enable them to deal with inquiries or complaints about their compliance. It is anticipated that credit reporting bodies will demonstrate their compliance with this obligation by, for example, developing and maintaining training programs, staff manuals, standard procedures and any other relevant documents that demonstrate awareness of, and compliance with, their obligations under the Division and the registered CR code. In addition, credit reporting bodies should be able to demonstrate that their business systems, such as their data management systems, comply with the requirements of the Division or the registered CR code.

Subclause (3) requires credit reporting bodies to have a policy dealing with their management of credit reporting information. The policy must be clearly expressed and up-to-date.

Subclause (4) provides a list of matters on which the policy must contain information. The list is not exhaustive and the policy can, and should where necessary to satisfy the obligation set out in subclause (3), contain additional information. The purpose of the list is to provide guidance to credit reporting bodies on information that the policy must contain which is likely to be directly relevant to individuals and their concerns about the information handling practices of credit reporting bodies. It is not intended that the policy set out matters such as detailed operational or administrative procedures or the processes of internal data management systems, nor is it intended that the policy establish technical data handling standards.

Subclause (5) requires credit reporting bodies to take reasonable steps to make the policy publicly available. Credit reporting bodies must take reasonable steps to make the policy available free of charge, and must make the policy available in an appropriate form – for example, on the website'.

Subclause (6) ensures that the policy is readily available to the public. While a credit reporting body may decide to make the policy available on their website, there may be circumstances where a person or body may wish to have the policy in a particular form – for example, in a different digital form that is more accessible for readers with a disability, or as a printed booklet. Following any such request, credit reporting bodies must take reasonable

steps to provide the person or body with a copy of their policy in the requested form. It is expected that a credit reporting body would not charge for access.

Subdivision C – Collection of credit information

Clause 20C Collection of solicited credit information

This provision is based on the obligations and structure of APP 3, modified to apply specifically to credit reporting bodies and their collection of credit information. The provision generally prohibits the collection of solicited credit information by credit reporting bodies, then sets out a series of exceptions to the prohibition. The primary source from which credit information is collected by credit reporting bodies is credit providers. The disclosure of credit information by credit providers to a credit reporting body is dealt with by clause 21D. However, the exceptions to the general prohibition on collection by credit reporting bodies set out other permitted circumstances in which credit reporting bodies can collect solicited credit information.

Taken together, clauses 20C and 21D prescribe the means by which credit information enters the credit reporting system. In the context of considering the data flows in the credit reporting system, these provisions deal with how credit information flows into the system. As discussed above in definitions, credit information comprises all of the basic data sets about the individual which are permitted in the credit reporting system and from which all other information in the system is wholly or partly derived.

Subclause (1) prohibits a credit reporting body from collecting credit information about an individual. Breach of this prohibition is subject to a civil penalty of 2000 penalty units.

Subclauses (2) to (6) deal with the exceptions to the prohibition in subclause (1).

Subclause (2) provides a general exception to the prohibition where the collection is required or authorised by or under an Australian law or a court or tribunal order.

Subclause (3) provides an exception for collection of credit information from a credit provider. This provision provides a link to the permitted disclosure by credit providers set out in clause 21D. However, the credit information can only be collected if the collection is done in the course of carrying on a credit reporting business. A credit reporting body is defined as agency or organisation (which for these purposes includes a small business) that carries on a credit reporting business. A credit reporting business may have other lines of business. This provision clarifies that credit information can only be collected from a credit provider if it is for the credit reporting business – this provision does not provide an exception to the prohibition on the collection of credit information for any other line of business that a credit reporting body may conduct. Finally, a credit reporting body is only permitted to collect identification information about an individual if it also collects, or already holds, another kind of credit information about the individual. The reference to credit information of another kind refers to the definition of credit information, which lists the kinds of information that can be collected. The purpose of this limitation is to prevent credit reporting bodies from compiling a data base that comprises identification information about individuals without any associated credit information. The purpose of the credit reporting system is not to provide an identification data base of individuals in Australia, but to assemble credit information which relates to the credit worthiness of individuals, as these terms are defined.

Subclause (4) sets out the circumstances in which credit reporting bodies are permitted to collect credit information from entities other than credit providers. Some kinds of credit information (for example, court proceedings information, personal insolvency information, or

publicly available information as described in the definition of credit information) may be available from entities other than credit providers and credit reporting bodies may wish to collect these kinds of credit information from those sources. In addition, there may be circumstances in which a credit provider has assigned debts owing to the credit provider to another entity that is not a credit provider, and a credit reporting body wishes to collect relevant credit information from the entity. It may also be the case that a credit reporting body wishes to make arrangements to collect credit information from another credit reporting body. Consistent with subclause (3), the collection of this credit information must be in the course of carrying on a credit reporting business.

Subclause (4) goes on to set a number of limitations on the collection of credit information from entities other than credit providers. These limitations are consistent with the limitations imposed upon the disclosure of credit information by credit providers in clause 21D. Because those entities which are not credit providers are not directly regulated by the credit reporting provisions, the only way in which the necessary limitations can be imposed on the flow of credit information into the credit reporting system is to restrict the collection of such information by credit reporting bodies.

Accordingly, the general restriction preventing the collection of credit information about an individual who is under 18 years old is stated in subclause (4)(a)(ii). In addition, subclause (4)(b) states that the credit information cannot relate to any act, omission, matter or thing that occurred or existed before the individual turned 18. This is to prevent the back-capture of past activity of an individual after they turn 18. In general terms, information about any credit related activity undertaken by a person before they turn 18 cannot be included in the credit reporting system (unless permitted by the exceptions to this general rule that follow). This means that, for example, an individual who obtains credit, repays the loan as required, and concludes the credit contract before they turn 18 will not have any information about that credit contract included in the credit reporting system. Similarly, if an individual defaults on credit before they turn 18 the default cannot be subsequently listed after the individual turns 18 if the credit has been terminated or otherwise ceases to be in force. However, subclause (5) states that the prohibition on collection of credit information about an individual before they turned 18 does not apply to identification information. This will allow, for example, the collection of prior addresses as permitted in the definition of identification information where the prior addresses relate to a time before the individual turned 18. In addition, subclause (6) states that the prohibition on collecting credit information about an individual before they turned 18 does not apply to consumer credit liability information that was entered into before the individual turned 18, so long as the consumer credit was not terminated or otherwise cease to be in force before the individual turned 18. The purpose of this exception to the general prohibition on collecting credit information about an individual before they turned 18 is to recognise that consumer credit liability information, as defined, includes information about the day the consumer credit is entered into, and this information, along with all the other consumer credit liability information, can be provided into the credit reporting system.

Subclause (4) also sets out two additional limitations on the collection of credit information by credit reporting bodies from entities other than credit providers. Subclause (4)(c) states that, if the information to be collected relates to consumer credit or commercial credit, the credit must have been provided, or applied for, in Australia. This is consistent with the general objective that the credit reporting system is only intended to provide information about credit in Australia, and should not contain information about the credit activities of individuals outside Australia. Subclause (4)(e) provides that repayment history information can only be collected from an entity that is not a credit provider where that entity is another Australian credit reporting body.

Subclause (7) states the general obligation, consistent with APP 3, that credit reporting bodies must only collect credit information by lawful and fair means.

Subclause (8) states that this provision only applies to credit information that is solicited by a credit reporting body. This is to distinguish the provision from situations where unsolicited credit information is received.

Clause 20D Collection of unsolicited credit information

This provision is based on the obligations and structure of APP 4, modified to apply specifically to credit reporting bodies and credit information.

Subclause (1) states that the credit reporting body that receives unsolicited credit information must determine whether the credit reporting body could have collected the information under clause 20C if they had solicited the information. Any use or disclosure for the purposes of making this determination is permitted by subclause (2). If the credit reporting body determines that it could have collected the credit information, subclause (3) makes clear that the obligations set out in clauses 20C to 20ZA apply to that collection. Subclause (4) states that the unsolicited credit information must be destroyed as soon as practicable if the credit reporting body determines that it could not collect the credit information, and imposes a civil penalty of 1000 penalty units for failure to comply with this requirement. However, there may be circumstances where the credit reporting body is required to retain the unsolicited credit information by or under an Australian law or a court or tribunal order. In these circumstances, subclause (5) permits the retention of the information.

Subdivision D – Dealing with credit reporting information etc

The provisions in Subdivision D relate to the next stage in the flow of information in the credit reporting system. Clauses 20C and 20D in Subdivision C dealt with the collection of credit information. Subdivision D now deals with credit reporting information. As defined, credit reporting information includes both credit information (collected by credit reporting bodies under clauses 20C or 20D) as well as CRB derived information about an individual. The provisions in the remainder of this division apply to this broader category of credit reporting information.

Clause 20E Use or disclosure of credit reporting information

Clause 20E sets out the general rules for the use or disclosure of credit reporting information by credit reporting bodies. This provision is based on the obligations and structure of APP 6, but has been significantly modified to apply specifically to credit reporting bodies and credit reporting information.

Subclause (1) establishes a general prohibition on the use or disclosure of credit reporting information about an individual by a credit reporting body. Breach of this prohibition is subject to a civil penalty of 2,000 penalty units. Subclauses (2) and (3) provide exceptions for this general prohibition.

Subclause (2) sets out the permitted uses, which are exceptions to the prohibition on using credit reporting information in subclause (1). A credit reporting body is generally permitted to use credit reporting information in the course of carrying on its credit reporting business. It is anticipated that this will allow the use of credit reporting information for matters such as data management, where this is done in the course of carrying on the credit reporting business. This would not permit a credit reporting body to use credit reporting information for any other business venture. Unlike APP 6, no secondary uses of credit reporting information by a credit reporting body are permitted. Only those uses expressly provided in subclause (2) and other provisions in this Division are permitted. In addition to the uses

permitted in subclause (2), the use of pre-screening assessments is dealt with by clause 20H and the use of de-identified credit reporting information is dealt with by clause 20M.

Paragraphs (2)(b) and (c) also permit a credit reporting body to use credit reporting information if the use is required or authorised by or under Australian law or a court or tribunal order, or the use is prescribed in the regulations. For example, the use of credit reporting information for certain identity verification purposes is specifically authorised, and regulated by, the *Anti-Money Laundering and Counter Terrorism Financing Act 2006*. The regulation-making power provides a means to permit any currently unforeseen but necessary uses that may arise in the future. Additional uses will be permitted where the use can be shown to be in the public interest as well as being for the benefit of the individuals whose credit reporting information would be used. Appropriate public consultation with all relevant stakeholders would be undertaken when considering whether regulations prescribing any additional uses should be prepared.

Subclause (3) sets out the permitted disclosures, which are exceptions to the prohibition on disclosing credit reporting information in subclause (1). Paragraph (3)(a) provides that a credit reporting body does not breach this provision if the disclosure is a permitted CRB disclosure in relation to the individual. Clause 20F sets out a table of permitted CRB disclosures, which identifies to whom a disclosure may be made and any related conditions around the disclosure.

The remaining paragraphs of subclause (3) set out specific permitted disclosures. Paragraph (3)(b) permits disclosures of credit reporting information to another Australian credit reporting body. This is consistent with subclause 20C(4), which allows the collection of credit information from entities other than credit providers. Paragraph (3)(c) permits disclosures to external dispute resolution schemes that have been recognised by the Information Commissioner and a credit reporting body or credit provider is a member of the scheme. This provision is intended to ensure that external dispute resolution schemes can access relevant credit reporting information, where appropriate, to assist in the resolution of complaints made by individuals about their personal information in the credit reporting system. Paragraph (3)(d) permits disclosures to enforcement bodies in relation to serious credit infringements (as defined). This provision will assist enforcement bodies in the investigation of alleged serious credit infringements. Paragraphs (3)(e) and (f) also permit a credit reporting body to disclose credit reporting information if the disclosure is required or authorised by or under Australian law or a court or tribunal order, or the disclosure is prescribed in the regulations. The regulation-making power provides a means to permit any currently unforeseen but necessary disclosures that may arise in the future. As stated above in relation to the regulation-making power for uses of credit reporting information, this power would be exercised where the disclosure is in the public interest, for the benefit of the individual, and following appropriate public consultation.

Disclosures under paragraphs (3)(a) (which permits the disclosures set out in the table in clause 20F) and (3)(f) (which permits disclosures under regulations, if any) are subject to an additional limitation if the disclosure is credit reporting information that includes, or was derived from, repayment history information. Subclause (4) provides that such information can only be disclosed if the credit provider to which it is being disclosed is a licensee (defined to mean a licensee under the National Consumer Credit Protection Act). This is intended to ensure that repayment history information, or credit reporting information that is derived from repayment history information, can only be disclosed to credit providers who are subject to responsible lending obligations under the National Consumer Credit Protection Act. This restriction extends to credit reporting information that was derived from repayment

history information because it is considered appropriate that credit providers who cannot access repayment history information should not be able to indirectly obtain the benefit of that information through the possibility that credit reporting bodies could provide credit reporting information that incorporates repayment history information in another form. The civil penalty for breach of subclause (4) is 2,000 penalty units.

Subclause (5) requires credit reporting bodies to make a written note of any disclosure of credit reporting information under subclause (3). Because subclause (3) includes disclosures which are permitted CRB disclosures under clause 20F, this means that written notes will need to be made of disclosures that fall within clause 20F. The purpose of requiring notes is to provide a record of all disclosures. To be an effective record, the written note should identify the date of the disclosure, the entity to which the credit reporting information was disclosed, the type of disclosure (including the specific provision under which the disclosure was authorised), the type of credit reporting information that was disclosed (where this is not clear from the type of disclosure), and any other relevant information (for example, that an individual's express consent to a disclosure under item 2 of the table at subclause 20F(1) was not in writing because of the circumstances set out in subclause 20F(2)). In relation to identifying the type of credit reporting information that was disclosed, a reader of the note should be able to determine whether all credit reporting information relating to the individual was disclosed, and if not, what types of credit reporting information were disclosed (for example, repayment history information). Written notes should be sufficiently associated with the credit reporting information of the relevant individual to ensure that individuals are able to obtain access to all written notes relating to their credit reporting information. Written notes do not themselves fall within the definition of credit information or credit reporting information, and so are not subject to the specific retention rules set out in clause 20W. However, as written notes would be personal information about an individual, a credit reporting body will be subject to the general obligations set out in the APPs in relation to the written notes of disclosures. As mentioned in the note to this subclause, other Acts provide that there are certain circumstances in which a note about a disclosure must not be made and those other Acts prevail over the obligation in this provision (which means complying with those other Acts will not be a breach of this provision). A breach of this provision attracts a civil penalty of 500 penalty units.

Subclause (6) provides that none of clause 20E applies to direct marketing. The purpose of this provision is to ensure that there is no inconsistency implied with clause 20G, which generally prohibits the use of credit reporting information for direct marketing.

Clause 20F Permitted CRB disclosures in relation to individuals

This provision sets out the permitted CRB disclosures that a credit reporting body is authorised to make under paragraph 20E(3)(a).

Subclause (1) states that a disclosure to an entity specified in the table is permitted subject to the conditions set out in the table. The table lists eight categories of permitted CRB disclosures. The conditions of each category of permitted CRB disclosure are intended to limit the disclosure to those circumstances that are necessary to achieve the purpose of each permitted disclosure.

The permitted CRB disclosures set out in the table are those disclosures which credit reporting bodies will most commonly make. When considered in the context of the information flows in the credit reporting system, this provision generally establishes the circumstances in which credit providers will receive information from the credit reporting system. At this point, information is flowing out of the credit reporting system to credit

providers. Credit providers do not have continuous access to credit reporting information. They can only obtain credit reporting information where the conditions set out in the table are satisfied.

The recipients of the information nominated in the table are also regulated in relation to the use that they can make of this information. Each disclosure permitted by a credit reporting body will subsequently be regulated as a use by the recipient. The disclosures in the table to credit providers are regulated as uses in clause 21H, while the disclosures to mortgage insurers and trade insurers are regulated as uses by clause 22C. Regulation of the credit reporting information in the hands of the recipient ensures that the use of the information is consistent with the purpose of the disclosure by the credit reporting body under this provision.

A disclosure under item 1 of the table to a credit provider is only permitted if it is for a consumer credit related purpose in relation to the individual about whom the credit reporting information is requested. The term 'consumer credit related purpose' is defined, and this means disclosure can only occur if credit reporting information is necessary to assess an application for consumer credit or to collect overdue payments in relation to credit provided by the credit provider to the individual.

A disclosure under item 2 of the table to a credit provider is only permitted for a commercial credit related purpose. This is a defined term and means disclosure can only occur if it is for the purpose of assessing an application for commercial credit or to collect overdue payments in relation to commercial credit provided to the individual. In addition, the disclosure can only occur if the individual expressly consents to the disclosure of the information to the provider for that purpose. Subclause (2) states that, as a general rule, the express consent of the individual must be given in writing. However, where the individual has not made the application for commercial credit to the credit provider in writing, it is not necessary for the individual's consent to be in writing. A requirement for express consent is included because the credit reporting system does not generally deal with commercial credit matters. The definition of credit information only permits very limited information about commercial credit to be included as part of an individual's credit information. It is recognised that a credit provider may generally find an individual's credit information useful in assessing an application for commercial credit. The requirement for express written consent ensures that the individual is aware that their credit information will be used for a non-consumer credit purpose.

A disclosure under item 3 of the table to a credit provider is only permitted for a credit guarantee purpose in relation to the individual, and the individual must expressly consent, in writing, to the disclosure for that purpose. 'Credit guarantee purpose' is a defined term, and means the purpose of assessing whether to accept the individual as a guarantor in relation to credit provided to, or applied for by, another person. In this context, it is the individual who is proposing to be the guarantor whose credit reporting information is being released, and the proposed guarantor must expressly consent to the disclosure in writing.

A disclosure under item 4 of the table of an individual's credit reporting information to a credit provider is only permitted if the credit reporting body is satisfied that a credit provider believes on reasonable grounds that the individual has committed a serious credit infringement (which is a defined term). The credit provider must demonstrate reasonable grounds for this belief to the credit reporting body to justify access under this provision.

A disclosure under item 5 of the table permits disclosure of credit reporting information to a current credit provider of an individual. A current credit provider is a credit provider that

holds credit liability information (a defined term) relating to consumer credit provided to the individual and that consumer credit has not been terminated or otherwise ceased to be in force. This provision allows credit reporting bodies to provide an individual's credit providers with default information (or where a payment of a default has occurred, payment information) about the individual. This provision will also allow credit reporting bodies to provide other relevant credit reporting information. However, when read with item 5 in the table at clause 21H, any credit reporting information disclosed under this provision can only be used by the recipient credit provider for the purpose of assisting the individual to avoid defaulting on the individual's consumer credit obligations to that credit provider.

A disclosure under item 6 of the table can be made to a securitisation entity that is defined as a credit provider by subclause 6J(1). Credit reporting information can be disclosed to such a credit provider only where the provider requests the information for a securitisation related purpose of the credit provider in relation to the individual. A securitisation related purpose is a defined term and refers to assessing the risk of purchasing, by means of a securitisation arrangement, credit that has been provided to the individual or to a person to whom the individual is or proposes to be a guarantor. The definition of the term also refers to assessing the risk in undertaking credit enhancement in relation to credit that has been provided to an individual (or a person to whom the individual is or may be a guarantor) through a securitisation arrangement.

A disclosure under item 7 may be made to a mortgage insurer (a defined term) where the credit reporting information is requested by the mortgage insurer for a mortgage insurance purpose in relation to the individual. The term 'mortgage insurance purpose' is defined.

A disclosure under item 8 may be made to a trade insurer (a defined term) where the credit reporting information is requested by the trade insurer for a trade insurance purpose (a defined term) in relation to the individual. However, in addition the individual must expressly consent in writing to the disclosure of the credit reporting information to the trade insurer for that purpose. This is consistent with the requirement for express consent for disclosures that relate to the assessment of commercial credit applications.

Clause 20G Use or disclosure of credit reporting information for the purposes of direct marketing

This provision generally prohibits the use or disclosure of credit reporting information for direct marketing purposes, then deals with pre-screening use and disclosures.

Subclause (1) expressly prohibits the use or disclosure of credit reporting information for the purposes of direct marketing. Breach of this provision is subject to a civil penalty of 2000 penalty units.

In general terms, subclause (2) permits the use by credit reporting bodies of credit information for pre-screening. Pre-screening is a direct marketing process by which direct marketing credit offers to individuals are screened against limited categories of credit information about those individuals to remove individuals from the direct marketing credit offer, based on criteria established by the credit provider making the offer, before the offers are sent. Generally, the process for pre-screening a direct marketing credit offer works as follows. The credit provider making the credit offer establishes the eligibility requirements for the direct marketing credit offer and provides the list of individuals about whom the pre-screening assessment will be made; the credit reporting body undertakes the pre-screening assessment and determines whether an individual is eligible consistent with those criteria; the credit reporting body discloses the pre-screening assessment to a mailing house which

conducts the direct marketing consistent with the pre-screening assessment, and then the pre-screening assessment is destroyed by the credit reporting body and the mailing house.

Subclause (2) sets out the conditions under which pre-screening can occur. The conditions are cumulative and all must be satisfied for the pre-screening to occur. Paragraph (2)(a) says that the credit provider who is doing the direct marketing must be an Australian credit provider (that is, have an Australian link as defined) and must be a licensee (that is, subject to responsible lending obligations). Paragraph (2)(b) states that the direct marketing must be about consumer credit that the credit provider provides in Australia, to ensure that the overall restriction on the use of the credit reporting system for Australian consumer credit is maintained.

Paragraph (2)(c) limits the categories of credit information that are available for pre-screening by excluding consumer credit liability information and repayment history information from use. As the stated purpose of pre-screening is to remove individuals from the direct marketing offer, it was considered that these two categories provide too much positive information about an individual's credit arrangements and hence are unnecessary to achieve the stated purpose of pre-screening. Limiting the types of credit information that are available for use is privacy enhancing.

Paragraph (2)(d) states that the credit reporting body must use the available credit information to assess whether or not the individual is eligible to receive the direct marketing offer of the credit provider. This must be read with subclause (3), which requires the credit reporting body to have regard to the eligibility requirements the credit provider nominates in relation to the pre-screening of the direct marketing credit offer. The assessment made by the credit reporting body under this paragraph is called a 'pre-screening assessment'. The process set out in this paragraph means that the credit provider itself does not receive any credit information in relation to its credit offer, nor does the credit provider undertake the pre-screening process itself. Pre-screening is conducted by the credit reporting body on the instructions of the credit provider.

Paragraph (2)(e) states that credit information about an individual can only be used for pre-screening where the individual has not made a request under subclause (5), which allows individuals to 'opt-out' of pre-screening. Paragraph (2)(f) requires the credit reporting body to comply with any additional requirements set out in the registered CR code in relation to pre-screening. It is expected that the registered CR code may deal with matters such as requirements by credit reporting bodies and recipients of pre-screening assessments to maintain audit trails of pre-screening activity and other process related matters. It is possible the entities that receive pre-screening information to be bound by the CR code, as the provisions in new Part IIIB on codes provide that the CR code may bind any entity to which Part IIIA (the credit reporting provisions) apply.

As stated above, subclause (3) modifies paragraph (2)(d). When setting criteria, the credit provider can only nominate criteria that remove individuals from the direct marketing credit offer.

Subclause (4) states that an assessment by a credit reporting body under paragraph (2)(d) is not credit reporting information about this individual. The assessment is called a 'pre-screening assessment' and subject to the specific rules set out in clauses 20H and 20J. As the assessment is not credit reporting information, it cannot be maintained as part of the individual's credit reporting information and cannot be disclosed, except as permitted by clause 20H.

Subclause (5) provides the opportunity for individuals to opt-out of having their credit information used for pre-screening of direct marketing credit offers. At any time an individual can request a credit reporting body that holds credit information about the individual not to use the credit information for pre-screening under subclause (2). Providing an opt-out option is consistent with the approach taken in APP 7 on direct marketing. Paragraph 20B(4)(e) expressly requires credit reporting bodies to have policies about the management of credit reporting information which deal with pre-screening and how an individual may make an opt-out request. A credit provider is required by clause 21C to expressly notify the individual, at or before the time of collection of personal information, the details of the credit reporting bodies which the credit provider deals with and any other matters specified in the registered CR code. It is expected that these notification requirements and the credit reporting body's privacy policy will give the individual sufficient opportunity to opt-out of any pre-screening of direct marketing credit offers. In general, the limitations placed upon the pre-screening process operate as privacy protections and, in the circumstances, an opt-out rule is considered appropriate. In the consumer credit regulatory environment, it appears that the *National Consumer Credit Protection (Home Loans and Credit Cards) Act 2011* imposes an opt-in model for the receipt of direct marketing of credit card limit increase invitations. It appears that the opt-in approach is not used elsewhere in the National Consumer Credit Protection Act and was chosen to address particular concerns around the marketing of credit card limit increases. While this approach was chosen in that particular circumstance under that Act, the opt-out approach for pre-screening is consistent with the privacy protections in place.

Subclause (6) prohibits a credit reporting body from charging an individual for making a request under subclause (5) or giving effect to the request.

Subclause (7) requires credit reporting bodies to make a written note of any use of credit information under subclause (2) for pre-screening. Written notes should be sufficiently associated with the credit reporting information of the individual to ensure that individuals are able to obtain access to all written notes relating to their credit reporting information. Written notes do not themselves fall within the definition of credit information or credit reporting information, and so are not subject to the specific retention rules set out in clause 20W. However, as written notes would be personal information about an individual, a credit reporting body will be subject to the general obligations set out in the APPs in relation to the written notes of disclosures. Breach of this obligation is subject to a civil penalty of 500 penalty units.

Clause 20H Use or disclosure of pre-screening assessments

This provision deals with the use and disclosure of pre-screening assessments, a defined term which refers to paragraph 20G(2)(d). This provision regulates the progression of the pre-screening process from the screening stage (dealt with in clause 20G) on to the process of issuing the screened direct marketing credit offers, by controlling the handling of the pre-screening assessment information. Information flows in the pre-screening process are essentially one-way – the credit provider is not given the results of the pre-screening process (referred to as the 'pre-screening assessment' in the Bill) and so cannot determine which individuals may have been excluded from the direct marketing credit offer as a result of the assessment. This is to ensure that credit providers are not able to target direct marketing to those people who they know have been excluded from their direct marketing offer. The purpose of pre-screening is purely to provide a process to remove individuals from direct marketing offers, not to allow credit providers to target identified individuals with direct marketing offers.

Subclause (1) generally prohibits the use or disclosure of a pre-screening assessment made by a credit reporting body. Breach of this provision is subject to a civil penalty of 2000 penalty units.

Subclause (2) provides an exception to the prohibition in subclause (1). This provision permits the credit reporting body to disclose, for the purposes of direct marketing, the pre-screening assessment to an Australian entity (that is, an entity which has an Australian link). However, the provision does not permit the disclosure of the pre-screening assessment back to the credit provider on whose behalf the assessment was made. The credit provider does not have any access to the pre-screening assessment. As the recipient of the assessment must be an entity, they will be subject to the APPs as well as the specific obligations set out in relation to pre-screening assessments. The entity (usually a mailing house) undertakes the direct marketing of the credit offer on behalf of the credit provider, consistent with the pre-screening assessment.

Subclause (3) requires the credit reporting body to make a written note of any disclosure under subclause (2). As with other written notes, the notes should be sufficiently associated with the credit reporting information of the individual to ensure that individuals are able to obtain access to all written notes relating to their credit reporting information. Written notes do not themselves fall within the definition of credit information or credit reporting information, and so are not subject to the specific retention rules set out in clause 20W. However, as written notes would be personal information about an individual, a credit reporting body will be subject to the general obligations set out in the APPs in relation to the written notes of disclosures. Breach of this obligation is subject to a civil penalty of 500 penalty units.

Subclause (4) establishes a general prohibition to any use or disclosure of the pre-screening assessment by the recipient of the assessment under subclause (2). Breach of this provision is subject to a civil penalty of 1000 penalty units.

Subclause (5) operates as an exception to the prohibition in subclause (4). This provision allows the recipient to use the pre-screening assessment for the purpose of doing the direct marketing by, or on behalf of, the credit provider.

Subclause (6) requires the recipient to make a written note of any use under subclause (5). It is expected that this written note would be accessible to the individual through the access provisions in the APPs. Breach of this obligation is subject to a civil penalty of 500 penalty units.

Subclause (7) makes clear that, if the recipient of the pre-screening assessment is an APP entity, then APPs 6, 7 and 8 do not apply in relation to the pre-screening assessment.

Clause 20J Destruction of pre-screening assessment

This provision deals with the destruction of pre-screening assessments. Subclause (1) states that an entity (which includes credit reporting bodies) that has possession or control of a pre-screening assessment must destroy the assessment if it is no longer needed for a purpose under clause 20H and the entity is not required by or under an Australian law or court or tribunal order to retain the assessment. The exception permitting retention where it is required by or under Australian law is also appropriate in these circumstances. Breach of this provision is subject to a civil penalty of 1000 penalty units.

Subclause (2) makes clear that, if the destruction obligation applies to an APP entity that is not a credit reporting body, APP 11.2 does not apply in relation to the pre-screening

assessment. The application of the APPs to credit reporting bodies in relation to pre-screening assessments has already been addressed in clause 20A.

Clause 20K No use or disclosure of credit reporting information during a ban period

This provision provides a mechanism for individuals to deal with potential fraud, including identity fraud, by controlling the disclosure of their credit reporting information in certain circumstances for the purpose of assessing applications for credit. In general terms, where an individual has reasonable grounds to believe that they have been, or are likely to be, the victim of fraud, they can request a credit reporting body not to use or disclose credit reporting information about the individual. There are limited exceptions to this general rule, and the provision also deals with the period of time for which the request remains active, and how to extend that period of time. The terms fraud and identity fraud are not defined. Activities that constitute identify fraud may change over time. Guidance on identity fraud may be available from law enforcement and crime prevention agencies.

This provision is linked to other provisions to provide a thorough response to identity fraud issues. Destruction of credit reporting information by the credit reporting body in cases of fraud is dealt with by clause 20Y. Clause 21F deals with credit providers and limits the disclosure of credit information to credit reporting bodies during a ban period. Essentially, if a credit provider is unable to obtain access to an individual's credit reporting information to assess an application for credit due to a ban period but proceeds to provide credit to a person purporting to be the individual, the credit provider cannot list any of the information about that credit as part of the individual's credit information (unless, as provided in the exception, the credit provider has taken reasonable steps to verify the individual's identity). This is intended to ensure that credit providers take reasonable steps to identify a person to whom they intend to provide credit during a ban period.

It is expected that further practical details around the operation of this provision would be covered in the registered CR code. Matters that may be covered include: notifying the individual of the effect of the ban period and the circumstances in which the individual should be notified that the ban period is ending; the extension of the ban period; notification of credit providers of the ban period; and other relevant matters.

Subclause (1) states that, where a credit reporting body holds credit reporting information about an individual, and the individual believes of reasonable grounds that they have been, or are likely to be, the victim of fraud (including identity fraud), then the individual can request the credit reporting body not to use or disclose their credit reporting information. Where this request is made, then despite any other provision of this Division, the credit reporting body must not use or disclose the credit reporting information during what is known as the ban period (a term that is further defined in subclauses (3) to (5)). Breach of this provision is subject to a civil penalty of 2000 penalty units. The individual must believe on reasonable grounds that they have been, or are likely to be, the victim of fraud. It is expected that this would generally mean that an individual who is able to explain why they believe they have been, or are likely to be, the victim of fraud would satisfy this requirement. Identity fraud can happen quickly and consequences for a victim of identity fraud can be significant. In this context, the purpose of this provision is to allow an individual who has been, or is likely to be, the victim of fraud to act quickly to try to ameliorate the risk of suffering losses. It is not expected that an individual would ordinarily need to, for example, present documentary evidence to support their belief.

The purpose of this provision is to limit the consequences of actual or suspected fraud on the individual. However, credit reporting bodies are not prevented from informing credit

providers of the fact that a ban period is in place in relation to an individual's credit reporting information. Informing credit providers of the ban period may assist them in preventing the perpetrator of the alleged fraud from causing further harm to the individual or others. It is expected that further procedural details around notification of credit providers of a ban period will be set out in the registered CR code.

Subclause (2) provides limited exceptions to the prohibition on use or disclosure of the individual's credit reporting information: where the individual expressly consents, in writing to the use or disclosure; or where the use or disclosure is required by or under an Australian law or court or tribunal order (note that this exception only operates where the use or disclosure is required and does not operate in situations where the use or disclosure may merely be authorised). Express consent by the individual in writing is provided as an exception to ensure that the individual is not adversely affected by the ban on the use or disclosure of their credit reporting information. An individual who, for example, had made, or was considering making, an application for credit would be able to provide express consent for the credit provider to obtain their credit reporting information from the credit reporting body. The credit provider would also need to take reasonable steps to identify the individual before relying on the consent.

Subclause (3) describes the operation of the ban period in relation to the credit reporting information of an individual that has satisfied subclause (1). The ban period starts when the individual makes the request in paragraph (1)(c) and ends 21 days after the day on which the request was made, or on the day after any extension under subclause (4) ends.

Subclause (4) permits the extension of the ban period after the initial 21 day period set out in subclause (3). The individual can, before the ban period ends, request the credit reporting body to extend the ban period. If an extension is requested, the credit reporting body must believe on reasonable grounds that the individual has been, or is likely to be, a victim of fraud. If the body forms such a belief, the body must extend the ban period by such period as it considers reasonable in the circumstances and give the individual written notification of the extension. Failure to comply with these requirements is subject to a civil penalty of 1000 penalty units. The difference from the initial request is that an extension can only be made if the credit reporting body forms a belief on reasonable grounds about the likelihood that the individual is, or may be, the victim of fraud. A credit reporting body could ask the individual to demonstrate the basis for their belief that they are, or may be, the victim of fraud. This would depend on the circumstances of each case, but would not necessarily require any court based evidence (such as the arrest of a person who is alleged to have committed the fraud). In some cases, the risk of fraud may continue for a significant period and the credit reporting body should make a judgement in the circumstances of the appropriate period of time for the extension. It is not intended that an individual would be placed under additional stress by the imposition of short extension periods that have to be regularly renewed if the circumstances do not warrant this approach. In this context, the registered CR code may provide more detail about the extension process.

Subclause (5) permits a ban period to be extended more than once under subclause (4).

Subclause (6) states that an individual who requests a ban period under paragraph (1)(c) or an extension of a ban period under paragraph (4)(b) should not be charged by the credit reporting body for making the request or giving effect to the request.

Clause 20L Adoption of government related identifiers

This provision is based on the obligations set out in APP 9(1), modified to apply specifically to credit reporting bodies.

Subclause (1) states that if a credit reporting body holds credit reporting information about an individual and that information is also a government related identifier of the individual, the credit reporting body must not adopt it as its own identifier of the individual. Breach of this provision is subject to a civil penalty of 2000 penalty units.

Subclause (2) provides an exception to the prohibition where the adoption of a government related identifier is required or authorised by or under an Australian law or a court or tribunal order.

Clause 20M Use or disclosure of credit reporting information that is de-identified

This provision deals with the use and disclosure of credit reporting information that has been de-identified for research purposes in relation to the assessment of credit worthiness of individuals. Generally, de-identified personal information is not regulated. The purpose of regulating de-identified credit reporting information is to clarify that such information can be used or disclosed in specified circumstances. The use and disclosure provisions for credit reporting agencies are prescriptive and do not permit any secondary uses or disclosures of credit reporting information. However, it appears that information from the credit reporting system has in the past been used for the purpose of conducting research (including statistical modelling and data analysis) relating to the assessment or management of credit. This research, where it is in the public interest, should be expressly permitted. Conducting research with de-identified personal information enhances privacy protection and appears to be consistent with existing industry practices. In addition, research is not a primary purpose of the credit reporting system and it is not appropriate to allow credit reporting information that identifies individuals to be used for research purposes. However, there can be concerns about the effectiveness of methods used to de-identify personal information and the risks of that information subsequently being linked again to individuals in a way that allows them to be identified. To ensure that the proposed research is consistent with these policy objectives and is appropriately limited in scope, the research will only be permitted where it complies with rules that the Commissioner may make about the use or disclosure of de-identified credit reporting information for research purposes. Permitting disclosure, as well as use, of the de-identified information is necessary to ensure that the credit reporting body can, for example, obtain expert assistance to conduct the research or is able to make the research available to credit providers, as well as other interested parties such as consumer credit advocates and privacy advocates.

Subclause (1) sets out a general prohibition on the use or disclosure of credit reporting information held by the credit reporting body that has been de-identified. Subclause (2) provides an exception to this prohibition where the use or disclosure of the de-identified information is for the purposes of conducting research in relation to the assessment of the credit worthiness of individuals. In addition, the credit reporting body must comply with rules made under subclause (3) by the Commissioner. Subclause (3) states that the Commissioner may make rules relating to the use or disclosure of de-identified information for the purposes of conducting research in relation to the assessment of the credit worthiness of individuals. Subclause (4) lists certain matters that, without limiting the Commissioner's power to make rules under subclause (3), the rules may deal with. The list identifies matters that are relevant to ensuring that the permitted research is for the general benefit of the public and in the public interest.

Subdivision E – Integrity of credit reporting information

20N Quality of credit reporting information

This provision is based on the obligations set out in APP 10, modified, and with additional provisions, to apply specifically to credit reporting bodies.

Subclause (1) provides that a credit reporting body must take such steps as are reasonable in the circumstances to ensure that the credit reporting information the body collects is accurate, up-to-date and complete. Subclause (2) applies to the use or disclosure of credit reporting information and includes an additional requirement of relevance. The requirement for information to be 'complete' does not require credit reporting bodies to enter into agreements with credit providers to ensure that all available credit information about the individual is disclosed, or for credit providers to disclose all available credit information to the body. The credit reporting body must take such steps as are reasonable in the circumstances to ensure that the credit reporting information the body uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant. The additional requirement of relevance means that the actual purpose of the use or disclosure must be considered. As all uses and disclosures of credit reporting information by credit reporting bodies are regulated by this Division, this will require careful consideration of the relevant provisions.

These provisions must be read in conjunction with the other provisions in this Division. Other provisions impose various restrictions on the collection, use and disclosure of some or all types of credit reporting information. For example, repayment history information is subject to specific restrictions to limit collection, use and disclosure to situations where credit providers are subject to responsible lending obligations by being licensees (as defined). In these circumstances, the disclosure, for example, of repayment history information will be restricted and this will limit the general obligation to disclose complete credit reporting information.

Subclause (3) sets out additional obligations imposed on credit reporting bodies to ensure they take appropriate steps to maintain the quality of credit reporting information. These obligations, which do not limit the general obligations set out in subclauses (1) and (2), require credit reporting bodies to enter into agreements with credit providers to ensure that credit information they disclose to the bodies is accurate, up-to-date and complete; a monitoring obligation, in the form of a requirement to ensure regular audits are conducted by an independent person to determine whether the agreements are being complied with; and an enforcement obligation, which requires bodies to identify and deal with suspected breaches of the agreements. It is expected that credit reporting bodies would have a range of enforcement mechanisms available to deal with breaches of the agreement, up to and including termination of the agreement with the credit provider, removing the credit provider from the credit reporting system. It is also expected that arrangements would be made to ensure an effective dispute resolution process was in place to deal with differences between bodies and credit providers in relation to the enforcement of the agreements. The purpose of these specific obligations is to ensure that both credit reporting bodies and credit providers take proactive steps in establishing practices which maintain the quality of credit information. Given that credit reporting bodies will play a central role in handling and managing credit information it is appropriate that they be charged with the responsibility to develop appropriate agreements. It is expected the registered CR code will include further practical details and obligations around the matters set out in subclause (3) to provide additional guidance to credit reporting bodies and credit providers.

Clause 20P False or misleading credit reporting information

This provision deals with using or disclosing false or misleading credit reporting information. It provides both an offence provision and a civil penalty provision to deal with this conduct. While civil penalty provisions have generally been used throughout the Bill to deal with situations in which breach of a provision warrants the imposition of a penalty, some kinds of conduct require the imposition of criminal penalties. Providing for both a criminal offence and a civil penalty in this provision gives the courts appropriate options to deal with the behaviour, depending on the circumstances of each case.

Subclause (1) states that a credit reporting body commits an offence if the body uses or discloses credit reporting information under this Division and the information is false or misleading in a material particular. Use or disclosure of unsolicited credit reporting information under subclause 20D(2) or the use or disclosure of information for consultation in response to an individual's request to correct their credit information under subclause 20T(4) are expressly excluded as these are circumstances where the information may be false or misleading and the credit reporting body either does not know, or is taking action to deal with, the errors. The penalty for this offence is 200 penalty units.

Subclause (2) sets out a civil penalty. A credit reporting body must not use or disclose credit reporting information under this Division if the information is false or misleading in a material particular. Once again, any use or disclosure under subclauses 20D(2) or 20T(4) is excluded from the civil penalty. The civil penalty for breach of this provision is 2000 penalty units.

Clause 20Q Security of credit reporting information

This provision is based on the obligations set out in APP 11, modified, and with additional provisions, to apply specifically to credit reporting bodies. The additional obligations imposed on credit reporting bodies in this provision are based on the additional obligations imposed on bodies by clause 20N to maintain the quality of credit information.

Subclause (1) provides that a credit reporting body that holds credit reporting information must take such steps as are reasonable in the circumstances to protect the information from misuse, interference and loss, and from unauthorised access, modification or disclosure. These are fundamental obligations and no exceptions are provided for these obligations.

Subclause (2) sets out additional obligations imposed on credit reporting bodies to ensure they take appropriate steps to maintain the security of credit reporting information. These obligations, which do not limit the general obligations set out in subclause (1), require credit reporting bodies to enter into agreements with credit providers to ensure that credit providers protect credit reporting information (that is, the category of information that they receive from credit reporting bodies) from misuse, interference and loss, and from unauthorised access, modification or disclosure. This is followed by a monitoring obligation, in the form of a requirement to ensure regular audits are conducted by an independent person to determine whether the agreements are being complied with, and an enforcement obligation, which requires bodies to identify and deal with suspected breaches of the agreements. It is expected that credit reporting bodies would have a range of enforcement mechanisms available to deal with breaches of the agreement, up to and including termination of the agreement with the credit provider, removing the credit provider from the credit reporting system. It is also expected that arrangements would be made to ensure an effective dispute resolution process was in place to deal with differences between bodies and credit providers in relation to the enforcement of the agreements. The purpose of these specific obligations is to ensure that both credit reporting bodies and credit providers take proactive steps in

establishing practices which maintain the security of credit information. Given that credit reporting bodies will play a central role in handling and managing credit information it is appropriate that they be charged with the responsibility to develop appropriate agreements. It is expected the registered CR code will include further practical details and obligations around the matters set out in subclause (2) to provide additional guidance to credit reporting bodies and credit providers.

Subdivision F – Access to, and correction of, information

Clause 20R Access to credit reporting information

This provision is based on the obligations set out in, and the structure of, APP 12, modified to apply specifically to credit reporting bodies. It is generally intended that access to credit reporting information should occur on the same terms as access to personal information held by an APP entity.

Subclause (1) states the general obligation that if a credit reporting body holds credit reporting information about an individual, the body must, on request by an access seeker, give the access seeker access to the information. The term access seeker is defined in clause 6L. In this context an access seeker means the individual to whom the credit reporting information relates, or a person who is assisting the individual deal with the credit reporting body, or an agent of the individual (that is, a person who is authorised in writing by the individual for the purpose of clause 20R, noting the exception provided for the National Relay Service in the definition of 'access seeker'). The term is subject to certain exceptions set out in the definition.

This provision permits the individual to obtain access to their credit reporting information. This includes both the credit information about the individual and the CRB derived information about the individual (for example, any credit scoring or analysis about the individual). While the individual can obtain access to the CRB derived information about them, this does not provide them with a right to access the methodology, data analysis methods, computer programs, or other information that the credit reporting body may use to manage their credit reporting information or to analyse their credit information to produce the CRB derived information.

Subclause (2) sets out exceptions to access. This list of exceptions has been deliberately modified and reduced from the list of exceptions set out in APP 12.3, on the basis that there is a significant public interest in ensuring individuals have access to their credit reporting information. These are the only grounds on which access can be refused. This provision states that the credit reporting body is not required to give access to the credit reporting information to the extent that: giving access would be unlawful (whether under the Privacy Act or another enactment); denying access is required or authorised by or under an Australian law or a court or tribunal order; or giving access would be likely to prejudice one or more enforcement related activities (a defined term – see schedule 1) by, or on behalf of, an enforcement body (defined in the Act).

Subclause (3) states that a credit reporting body must respond to the request for access within a reasonable period, but not longer than 10 days, after the request is made. It is considered that 10 days is a sufficient maximum period to provide access to an individual's credit reporting information and it is expected that reasonable access would ordinarily occur well within the 10 day period. The business of credit reporting bodies is handling and managing credit reporting information about individuals, so it is expected that bodies will have developed efficient systems to provide ready access to individual's seeking their credit reporting information.

Subclause (4) deals with the means of access. It states that, if a credit reporting body gives access, the access must be given in the manner set out in the registered CR code.

Subclauses (5) and (6) deal with access charges and requires credit reporting bodies to provide individuals with free access to their credit reporting information once every 12 months, on request of the access seeker. Subclause (5) states that the credit reporting body must not charge an access seeker for making a request or for access if a request has not been made to the body in the previous 12 months. Subclause (6) provides that, if subclause (5) does not apply, any charge by the credit reporting body for giving access must not be excessive and must not apply to the making of the request. This is the same test that applies under APP 12.8.

It is considered that credit reporting information is a particularly significant kind of personal information. As credit reporting information is used for matters relating to an individual's credit related activities where errors or omissions may have significant consequences for the individual, it is essential that the individual be able to obtain free access on a reasonably regular basis. It is considered that free annual access should generally be sufficient. However, there may be circumstances where an individual requires more regular access in a 12 month period, for example where the individual is the victim of fraud or identity fraud. Credit reporting bodies are not required to charge in every instance after the first free access in 12 months and it is expected that bodies will be flexible in the application of any charges for access.

Subclause (7) sets out the process of providing notice to the access seeker where access is refused. It provides that, where access is refused because of subclause (2) (which sets out the only exceptions to access), the credit reporting body must give the access seeker a written notice that sets out the reasons for the refusal. The obligation to provide reasons is limited to the extent that it would be unreasonable to do so, having regard to the grounds for the refusal. For example, where access to some of an individual's credit reporting information is refused because it may prejudice an enforcement related activity, it may be unreasonable to set out the details of the law enforcement activity or even that the law enforcement activity has provided the basis for restricting access to a part of the individual's credit reporting information.

Subclause (7) goes on to provide that the written notice provided to the access seeker must inform the access seeker that, if they are not satisfied with the response to the request, they may access a recognised external dispute resolution scheme of which the body is a member (and provide contact details for that scheme) or make a complaint to the Commissioner under Part V of the Act.

Clause 20S Correction of credit reporting information

Clauses 20S, 20T and 20U are based on the obligations set out in APP 13, modified, and with additional provisions, to apply specifically to credit reporting bodies. Read together, these three provisions set out a correction process that provides individuals with specific rights and deal with matters that are particularly important in the context of credit reporting, such as providing evidence to substantiate disputed personal information in the credit reporting system. Importantly, individuals are able to request the correction of their personal information that may not be held by the credit reporting body, requiring the credit reporting body to consult with the appropriate credit reporting body or credit provider. This imposes a specific obligation on bodies and credit providers to assist individuals to correct their personal information, no matter whom it is held by in the credit reporting system. This means that the credit reporting body or credit provider to which the individual first makes a

correction request must deal with that request and assist the individual to have their personal information corrected. The industry participants in the credit reporting system derive significant benefits from the availability of information about individuals in the system and it is considered appropriate that they take on obligations to assist individuals to correct their information. These provisions are mirrored by clauses 21U, 21V and 21W which impose similar obligations on credit providers.

Clause 20S sets out the general obligations on credit reporting bodies to correct credit reporting information. The correction obligation is expressly linked to the obligations on credit reporting bodies to ensure the quality of the credit reporting information they maintain. Subclause (1) provides that a credit reporting body must take reasonable steps (if any) to correct credit reporting information that is inaccurate, out-of-date, incomplete, irrelevant or misleading. Correction should take into account the purpose for which the information is held. The purpose of holding information will depend on the provisions of this Division and the definitions, and this will then inform decisions about whether information may be inaccurate, out-of-date, incomplete, irrelevant or misleading (note that if at least one of these descriptions can be applied to an individual's credit reporting information it must be corrected). For example, credit information may include an individual's current address and up to two previous addresses in the previous five years, if any. Holding the previous addresses does not mean that the credit reporting body has out-of-date information. However, address information may become out-of-date if, for example, the individual moves from their current address and the credit reporting body is made aware of this change, as the body will now be required to up-date the address information.

Subclause (2) states that a credit reporting body who has corrected credit reporting information that has previously been disclosed under this Division (with the exception of disclosure in relation to unsolicited information under subclause 20D(2) and disclosure to consult on a correction request under subclause 20T(4)) must, within a reasonable period, give each recipient of the information written notice of the correction. This obligation is to ensure that other recipients are aware of the correction and can take appropriate action to up-date their own records. As recipients of an individual's credit reporting information may be making credit related decisions of significance for the individual, it is important that any corrections are transmitted quickly and efficiently. It is expected that the registered CR code will deal with notification periods and procedures.

Subclause (3) provides that the obligation for written notice under subclause (2) does not apply if it is impracticable for the credit reporting body to give the notice or the credit reporting body is required by or under an Australian law, or a court or tribunal order, not to give the notice. It is expected that it would generally always be practicable for a credit reporting body to give the notice, as bodies must make written notes of any disclosures and they will also have agreements in place with the recipients of the information, for example to implement the requirements of subclause 20Q(2) on security. However, there may be circumstances where it is impracticable to provide the notice, for example where a credit provider has ceased trading.

Clause 20T Individual may request the correction of credit information etc

This provision sets out the process by which an individual may request the correction of certain personal information about them which is held in the credit reporting system. An individual is able to make a request for the correction of their information to a credit reporting body and the body must, if it does not hold the information or cannot be satisfied that the information should be corrected, take steps to consult another body or a credit provider to assist in resolving the individual's request.

Subclause (1) provides that an individual may request a credit reporting body to correct specified kinds of personal information in the credit reporting system if the body holds at least one of the specified kinds of personal information. The personal information about the individual that may be subject to a correction request may be credit information, CRB derived information, or CP derived information. While a credit reporting body will not hold CP derived information, the provision permits an individual to make a correction request about this kind of information to the body.

Subclause (2) states the obligation to correct the personal information if the credit reporting body is satisfied that it is inaccurate, out-of-date, incomplete, irrelevant or misleading. The correction must be made within 30 days from the day the request is made, or such longer time as the individual agrees in writing. It is expected that the registered CR code will deal in greater detail with the process around which extensions of time to respond to correction requests are proposed to the individual. However, it is generally expected that most requests for correction should be resolved within the 30 days specified in this provision. The period of 30 days has been specified to provide adequate time for consultation to occur under subclause (3), so the fact that consultation is required should not in itself be grounds for a body to request that the individual agree to a longer period for consideration of the correction request. Where consultation is not required, it is expected that the correction request would ordinarily be considered and resolved well within the 30 days. The correction and complaint processes have been streamlined so that an individual can lodge a complaint with the Commissioner or a recognised external dispute resolution service immediately upon receiving notice of a refusal to make the requested correction under clause 20U. Accordingly, it is considered that a maximum period of 30 days in all but unusual cases should not present an unreasonable delay for the individual to have their correction request considered and resolved.

Where the personal information is corrected by the credit provider after consultation with another credit provider, then the notice obligations set out in clause 21W will operate. Any interested party consulted must be given notice of the correction. Those interested parties would be required to correct any personal information they hold or maintain to which the notice of correction relates by the operation of clause 20S (for a credit reporting body) or clause 21U (for a credit provider), which requires bodies or providers to ensure certain personal information they hold or maintain is not inaccurate, out-of-date, incomplete, irrelevant or misleading.

Subclause (3) deals with the process where the credit reporting body must consult so that it can be satisfied of the matter raised in the correction request. A credit reporting body may consult an interested party, which is either or both of another credit reporting body or a credit provider about the individual's request. However, the credit reporting body can only consult an interested party that has an Australian link, consistent with the limitation of the credit reporting system to Australia.

Subclause (4) authorises the use or disclosure of personal information about the individual for the purposes of consultation under subclause (3). As this information is being used or disclosed because it may not be correct, exceptions exist in other provisions in relation to quality obligations.

Subclause (5) states that the credit reporting body must not charge the individual for the making of the correction request or for correcting the information.

Clause 20U Notice of correction etc must be given

This provision sets out the notice requirements that apply where the credit reporting body corrects, or does not correct, an individual's personal information.

Subclause (1) states that this provision applies if an individual requests a credit reporting body to correct personal information under clause 20T.

Subclause (2) deals with notice requirements where a credit reporting body has corrected the individual's personal information. The credit reporting body must, within a reasonable time, give written notice of the correction to the individual, to any interested party that the body consulted about the individual's correction request, and, where the information has been previously disclosed, to each recipient of the information (except where the disclosures were in relation to unsolicited information under subclause 20D(2) or the correction request under subclause 20T(4) – in the latter case, anyone consulted must in any event be given written notice). However, subclause (4) states that notice of all recipients is not necessary if it is impracticable for the credit reporting body to give the notice. It is expected that it would generally always be practicable for a credit reporting body to give the notice, as bodies must make written notes of any disclosures and they will also have agreements in place with the recipients of the information, for example to implement the requirements of subclause 20Q(2) on security. It may be impracticable to give notice in situations where, for example, the recipient of the information has ceased trading.

Subclause (3) deals with notice requirements where a credit reporting body does not correct the personal information as requested. The credit reporting body must, within a reasonable time, give the individual written notice: stating that the correction has not been made; setting out the body's reasons for not correcting the information; and informing the individual that, if they are not satisfied with the body's response to the request, the individual may access a recognised external dispute resolution scheme of which the body is a member or make a complaint to the Commissioner under Part V of the Act. When the body sets out its reasons for not correcting the information, the body is required to include evidence substantiating the correctness of the information. The kind of evidence that might substantiate the correctness of the information will depend on the circumstances and the kind of credit reporting information that is the subject of the correction request. For example, evidence to substantiate a default listing should show that all the elements of the definition of default have been satisfied, including evidence around the timing the notice requirements, and other such matters. Given that a default listing has a significant impact upon an individual's credit worthiness, information about the steps taken by the credit provider to satisfy the requirements of the default definition would be necessary, as well as other relevant evidence. This substantiation requirement means that the onus of proving the correctness of information that has been challenged by an individual rests with the body (which, through the consultation requirements in clause 20T, can obtain substantiation evidence from another body or credit provider). It is expected that this substantiation requirement will assist in resolving disputes quickly and efficiently, because if evidence substantiating the information cannot be produced it is very unlikely that the body would not be satisfied that the information should not be corrected as requested by the individual. In such circumstances the general obligations to maintain accurate, up-to-date and complete information will operate in support of the obligations to correct the information.

Subclause (5) sets a general exception to the notice obligations in subclauses (2) and (3) if the credit reporting body is required by or under an Australian law or a court or tribunal order not to give the notice.

Subdivision G – Dealing with credit reporting information after the retention period ends etc

Clause 20V Destruction etc. of credit reporting information after the retention period ends

Generally, personal information should be destroyed if it is no longer necessary for the purpose for which it was collected. The very specific nature of the personal information in the credit reporting system and the significant privacy sensitivities around this personal information for individuals means that rules are necessary to limit the retention of the information to specific periods of time and to ensure the destruction, or de-identification, of certain kinds of personal information.

This provision sets out the rules requiring the destruction of credit reporting information after the retention period for the information has ended. The retention periods are specified in clauses 20W and 20X. There are different retention periods for different kinds of credit reporting information. The requirement to destroy information applies to the particular information for which the retention period has ended. This means that destruction obligations for different kinds of credit reporting information of an individual will require continual monitoring to ensure compliance with the destruction obligations.

Subclause (1) sets out the application rule for this provision. The provision applies if the credit reporting body holds credit reporting information about an individual and the retention period ends. However, as indicated in the note, there is no retention period for identification information or credit information that as specified in paragraph 6N(k), which refers to certain kinds of publicly available information. Identification information is not subject to a specific retention period because it is necessary to identify the individual in relation to the other kinds of credit information. However, where a credit reporting body is left with only identification information about an individual because all other information has been destroyed consistent with this provision, the credit reporting body can no longer collect any updated identification information under clause 20C. It is expected the remaining identification information would be destroyed consistent with the obligations to maintain up-to-date records.

Different destruction rules apply to different credit information and CRB derived information (which together make up the credit reporting information). Where the retention period for credit information has ended, subclause (2) requires the information to be destroyed or de-identified within one month of the end of the retention period. Failure to comply with this obligation is subject to a civil penalty of 1000 penalty units. Subclause (3) provides an exception to the destruction rule where, immediately before the retention period ends, there is a pending correction request or a pending dispute (under the complaints arrangements in Division 5 or Part V of the Act) in relation to the credit information. Failure to comply with these exceptions is subject to a civil penalty of 500 penalty units. Subclause (4) provides an exception from the destruction rule if the credit reporting body is required by or under an Australian law or a court or tribunal order to retain the information.

Subclause (5) sets out the destruction rule for CRB derived information. A credit reporting body must destroy, or de-identify, any CRB derived information that was derived from the individual's credit information in the circumstances described. Where the CRB derived information is derived from two or more kinds of credit information, and at least one of those kinds of credit information must be destroyed or de-identified because the retention period has ended, then the CRB derived information must also be destroyed or de-identified at the same time. The effect of this rule is that the retention period for CRB derived information will always be linked to the kind of credit information that has the shortest retention period

and which was used to derive the CRB derived information. For example, CRB derived information that is derived in part from repayment history information will be subject to the two year retention period for that kind of information, irrespective of whether the other kinds of credit information also used to derive the CRB derived information had longer retention periods. In all other situations, paragraph (5)(b) provides that the CRB derived information is destroyed or de-identified at the same time as the credit information from which it is derived is destroyed or de-identified. This rule applies to those situations where the CRB derived information is derived form only one kind of credit information. Failure to comply with any of the obligations in this subclause is subject to a civil penalty of 1000 penalty units.

Subclause (6) provides an exception to the destruction rule for CRB derived information where, immediately before the retention period ends, there is a pending correction request or a pending dispute (under the complaints arrangements in Division 5 or Part V of the Act) in relation to the CRB derived information. Failure to comply with these exceptions is subject to a civil penalty of 500 penalty units. Subclause (7) provides an exception from the destruction rule for CRB derived information if the credit reporting body is required by or under an Australian law or a court or tribunal order to retain the information.

Clause 20W Retention period for credit information – general

Clause 20W sets out the retention periods for credit information held by a credit reporting body that is not personal insolvency information (which is dealt with in clause 20X). The items in the table describe the different kinds of credit information and the retention period for that information. As noted above, no retention period is specified for credit information that is identification information about an individual or credit information that is specified kinds of publicly available information.

Item 1 of the table sets the retention period for consumer credit liability information, a defined term, at 2 years from the day on which the consumer credit to which the information relates is terminated or ceases to be in force. This means consumer credit liability information can be retained for as long as the consumer credit to which it relates continues to run, and then for two years after that consumer credit has been terminated. In some circumstances, depending on the type of credit, an individual may have no further repayment obligations but the credit may remain available for the individual to use at a later date. This type of credit product would continue to be in force while credit remains available, and the relevant consumer credit liability information could continue to be held, until such time as the credit product is clearly terminated by closing the credit product so that credit is no longer available to the individual. At that point the two year retention period would commence.

Item 2 of the table sets the retention period for repayment history information, a defined term, at 2 years from the monthly payment to which the information relates is due and payable. This means that there is a rolling two year retention period for repayment history information. Information on any particular monthly payment can be held for no more than two years.

Item 3 of the table sets the retention period for information requests (as described in paragraph 6N(d)) and the type and amount of credit sought in an application (as described in paragraph 6N(e)) at 5 years from the day on which the information request to which the information relates is made.

Item 4 of the table sets the retention period for default information (a defined term) at 5 years from the day that the credit reporting body collects the information. It is necessary to link the retention period to the collection by the body because there is no other precisely defined date that is readily available to the credit reporting body.

Item 5 of the table sets the retention period for payment information (a defined term) at 5 years from the day on which the default information to which the payment relates is collected by the credit reporting body. As the payment information directly relates to the default its retention is linked to the default. It would not be possible to allow retention for a longer period (for example, retention for 5 years from the date of the payment) as this would effectively provide notice of the existence of a prior default even after the default itself could no longer be retained.

Item 6 of the table sets the retention period for new arrangement information as defined in subclause 6S(1) at 2 years from the day that the credit reporting body collects the default information to which the new arrangement relates.

Item 7 of the table sets the retention period for new arrangement information as defined in subclause 6S(2) at 2 years from the day that the credit reporting body collects the information about the opinion to which the new arrangement information relates.

Item 8 of the table sets the retention period for court proceedings information at 5 years from the day judgement to which the information is made or relates is made or given. Note that the date of judgement may be earlier than the date that the judgement is reported or reasons published.

Item 9 of the table sets the retention period for information under paragraph 6N(l) that is an opinion of a credit provider that an individual has committed a serious credit infringement (a defined term) at 7 years from the day the credit reporting body collects the information.

Clause 20X Retention period for credit information – personal insolvency information

Clause 20X sets out the retention periods for credit information that is held by a credit reporting body. The items in the table describe the different kinds of personal insolvency information and the retention period for that information. For each kind of personal insolvency in the table two retention periods are given, the first retention period counted from the start of the personal insolvency (and in each case is 5 years) and the second retention period counted from the end of the personal insolvency (and the retention period varies depending on the type of personal insolvency). In each case, the later of the two retention periods is the operative period. The reason for including a retention period for the end of each kind of personal insolvency is to recognise the significant differences between the kinds of personal insolvency arrangements. Depending on the kind of arrangement that an individual has entered, they may have made significant efforts to meet their obligations under the arrangement, while other individuals may have made no efforts. These differences should be recognised in determining an individual's credit worthiness. The minimum period for the retention of any kind of personal insolvency information will be 5 years, as it is considered that this is an appropriate period to provide information to credit providers to allow then to assess credit risk but to then allow individuals to have the opportunity of a fresh start to their financial affairs at the end of this period. However, the operation of the retention periods means that in appropriate cases the personal insolvency information may be retained for a longer period depending on the retention period permitted at the end of each kind of personal insolvency.

Item 1 of the table sets the retention period for information about the bankruptcy of an individual at the later of 5 years from the day the individual becomes bankrupt, or 2 years from the day the bankruptcy ends.

Item 2 of the table sets the retention period for information about a personal insolvency agreement (other than an agreement covered by item 3 of the table) at the later of 5 years

from the day on which the agreement is executed, or 2 years from the day the agreement is terminated or set aside.

Item 3 of the table sets the retention period for information about a personal insolvency agreement in relation to which a certificate has been signed under section 232 of the Bankruptcy Act at the later of 5 years from the day on which the agreement is executed, the day on which the certificate is signed.

Item 4 of the table sets the retention period for information about a debt agreement (other than an agreement covered by item 5 of the table) at the later of 5 years from the day the agreement starts, or 2 years from the day the agreement is terminated, or the whole agreement is declared void, under the Bankruptcy Act.

Item 5 of the table sets the retention period for information about a debt agreement that ends under section 185N of the Bankruptcy Act at the later of 5 years from the day the agreement starts, or the day on which the agreement ends.

Subclause (2) provides special rules for the retention of information of debt agreement proposals under the Bankruptcy Act. Special retention rules are required because proposals are not yet debt agreements and there are various things that may happen to proposals under the Bankruptcy Act. As soon as one of the things happens in relation to the debt agreement proposal as specified in paragraphs (a) to (d) the retention period ends.

Subclause (3) provides a special rule for the retention of personal insolvency information relating to a direction given, or an order made, under section 50 of the Bankruptcy Act, which deals with the control of certain property. The retention period ends on the day the control of the property to which the direction or order relates ends.

Subclause (4) provides a special rule for the retention of personal insolvency information that relates to an authority signed under section 188 of the Bankruptcy Act. The retention ends on the day on which the property to which the authority relates in no longer subject to control under Division 2, Part X of that Act.

Subclause (5) states an interpretation rule, which ensures that expressions used in this provision and in the Bankruptcy Act have the meaning set out in that Act.

Clause 20Y Destruction of credit reporting information in cases of fraud

Clause 20Y sets out a special destruction rule for information in cases of fraud. Clause 20K provides rules dealing with the use or disclosure of credit reporting information where an individual has been, or is likely to be, the victim of fraud. In cases where the individual has been the victim of fraud and consumer credit was provided to someone other than the individual, the individual should not continue to have information about that fraudulently obtained consumer credit maintained as part of their credit reporting information. However, as the information is about consumer credit that was supplied to someone purporting to be the individual, there may be uncertainty around how to deal with this information in the context of the rules set out in clauses 20N (about the quality of credit reporting information) and 20P (prohibiting the maintenance of false or misleading credit reporting information). This provision sets out special rules to deal with this situation.

Subclause (1) sets out the circumstances under which this provision applies. The credit reporting body must hold credit reporting information about an individual. The information must relate to consumer credit that has been provided by a credit provider to the individual, or a person purporting to be the individual. Finally, the body must be satisfied that the individual has been a victim of fraud and that the consumer credit was provided as a result of that fraud. While it is for the body to be satisfied of these matters, the evidence necessary to

satisfy the body of these matters should be appropriate in the circumstances. For example, it is not expected that court-based evidence would be necessary in every case before the body was satisfied of these matters. The appropriate evidence will depend on the circumstances of the fraud.

Where the requirements of subclause (1) have been satisfied, subclause (2) provides that the credit reporting body must destroy the credit reporting information. Within a reasonable period of time after the information is destroyed, the body must also give the individual a written notice stating that the information has been destroyed and informing the individual that any third parties which received the information will be notified of the information's destruction (as required by subclause (4)). The body must also give the credit provider that provided the consumer credit as a result of the fraud a written notice stating that the information has been destroyed. Breach of this provision is subject to a civil penalty of 1000 penalty units.

Subclause (3) sets out an exception to the destruction requirement in subclause (2). The requirements of subclause (2) do not apply if the credit reporting body is required by or under an Australian law or a court or tribunal order to retain the credit reporting information.

Subclause (4) sets out notice obligations about the destruction of the information to third parties. Where information has been destroyed under subclause (2), and the credit reporting body has previously disclosed the information to one or more recipients under Subdivision D of this Division, the body must within a reasonable period after the destruction notify those recipients of the destruction and that the body is satisfied the individual was a victim of fraud the consumer credit was provided as a result of that fraud. This is a general obligation to notify all recipients and the individual does not need to request notification of third parties. Breach of this provision is subject to a civil penalty of 500 penalty units. Credit reporting bodies will have retained written notes of any disclosures of the information, as required by various provisions in Subdivision D, which will assist them to comply with this obligation. Given the significance of credit reporting information to individuals and that decisions about an individual's credit worthiness may be made based on that information in the future, it is important that notification of all previous recipients occurs so that they can satisfy their obligations to maintain the quality of the credit reporting information that they hold.

Subclause (5) provides an exception to subclause (4). The requirements of subclause (4) do not apply if the credit reporting body is required by or under an Australian law or a court or tribunal order not to give the notification.

Clause 20Z Dealing with information if there is a pending correction request etc

Clause 20Z sets out rules to deal with situations where there is a pending correction request or a pending dispute in relation to credit reporting information that may otherwise be subject to destruction under clause 20V. In these circumstances it would not be appropriate to destroy the information. However, given that the retention would, but for the operation of these exceptions, be contrary to the destruction obligations, it is important that the Commissioner be informed of the situation and have the opportunity to issue directions about what must be done with the information. There is no similar provision for credit providers because they do not have any specific destruction obligations like those set out in clause 20V for credit reporting bodies.

Subclause (1) sets out the application of the provision. The credit reporting body must hold credit reporting information about the individual and either subclause 20V(3) or 20V(6) must apply in relation to the information. Subclause (2) requires the credit reporting body to notify the Commissioner as soon as practicable of this situation. Breach of this notification

requirement is subject to a civil penalty of 1000 penalty units. Subclause (3) prohibits any use of disclosure of this information, breach of which is subject to a civil penalty of 2000 penalty units. However, subclause (4) permits use or disclosure of the information if it is for the purposes of the pending correction request, or pending dispute, in relation to the information. Use or disclosure if the information is also permitted if the use or disclosure is required by or under an Australian law or court or tribunal order. If any use or disclosure occurs under subclause (4), then subclause (5) requires a written note to be made of that use or disclosure, subject to a civil penalty of 500 penalty units. This is consistent with the general approach of requiring credit reporting bodies to make written notes of any uses or disclosures of credit reporting information.

Subclause (6) gives the Commissioner the power to direct, by legislative instrument, that the credit reporting body destroy the information, or ensure it is de-identified, by a specified day. This power may be exercised by the Commissioner in appropriate circumstances to resolve the issue of whether the information should be destroyed or retained. For example, in some instances an individual may agree to the destruction of the information without resolving their correction request on the basis that the information will no longer appear as part of their credit reporting information or have any impact upon decisions about their current or future credit worthiness. Subclause (7) states that a credit reporting body must comply with a direction by the Commissioner given under subclause (6), and failure to do so is subject to a civil penalty of 1000 penalty units.

Subclause (8) clarifies the relationship of this provision to clause 20M, which deals with the use and disclosure of de-identified credit reporting information. If a credit reporting body is directed by the Commissioner to de-identify the credit reporting information under subclause (6) then clause 20M will apply to that de-identified information.

Clause 20ZA Dealing with information if an Australian law etc requires it to be retained

Clauses 20V and 20Y provide that credit reporting bodies must not deal with information in the ways otherwise specified in those provisions if they are required by or under an Australian law or a court or tribunal order not to so deal with the information. Accordingly, clause 20ZA provides rules for how credit reporting bodies are to deal with any information that is subject to these directions by another Australian law or court or tribunal order.

Subclause (1) sets out the application of the provision. This provision applies if a credit reporting body is not required to: destroy or de-identify credit information under subclause 20V(2) because of subclause 20V(4); destroy or de-identify any CRB derived information under subclause 20V(5) because of subclause 20V(7); or destroy credit reporting information under subclause 20Y(2) because of subclause 20Y(3).

If subclause (1) applies, subclause (2) states that the credit reporting body must not use or disclosure the information, breach of which is subject to a civil penalty of 2000 penalty units. Subclause (3) provides an exception from this general rule to permit any use or disclosure that is required by or under an Australian law or a court or tribunal order. Subclause (4) requires the body to make a written note of any such use or disclosure, consistent with the general policy of requiring bodies to note uses or disclosures. This is subject to a civil penalty of 500 penalty units.

Subclause (5) states that the obligations in relation to the integrity of information set out in Subdivision E (with one exception) do not apply in relation to the use or disclosure of the information. However, the security obligations in clause 20Q continue to apply. Subclause (6) states that the access and correction obligations set out in Subdivision F do not apply in

relation to the information. The purpose of these provisions is to clarify the application of these obligations to this information. If another Australian law or court or tribunal order requires the credit reporting body to do, or not do, certain things in relation to the information, it would be inappropriate to apply the full set of obligations to this information.

Division 3 – Credit providers

Subdivision A – Introduction and application of this Division

Clause 21 Guide to this Division

This provision provides a guide to the Division.

Clause 21A Application of this Division to credit providers

Clause 21A states that the Division only applies to credit providers in relation to: credit information; credit eligibility information; and CRB derived information.

Credit reporting information that is disclosed by credit reporting bodies to credit providers becomes credit eligibility information (which also includes CP derived information) in the hands of credit providers. For this reason credit providers are regulated in relation to credit eligibility information, rather than credit reporting information. Credit information is also regulated because credit providers have a dual role of both supplying credit information into, and collecting credit reporting information from, the credit reporting system.

This Division provides requirements that apply to credit providers in relation to these categories of information. While the APPs are completely replaced by the obligations for credit reporting bodies in Division 2, a different approach is taken for credit providers. The requirements for credit providers set out in Division 3 may apply in addition to the APPs (where a credit provider is an APP entity). Where any provision in this Division modifies or replaces an APP the relationship with the relevant APP will be made expressly clear in that provision. Other provisions impose obligations that do not directly relate to the APPs and so are additional to the APP obligations. Where an APP is not referred to in this Division then that APP will continue to apply to any information regulated by this Division and to credit providers that are APP entities in relation to that information. For example, this Division does not specifically regulate the collection of the kinds of personal information that are included in the definition of credit information. This means that APP 3 (dealing with the collection of solicited information) and APP 4 (dealing with the collection of unsolicited information) apply as appropriate and without modification to credit providers that are APP entities.

Credit providers have obligations in relation to these three categories of information. While a credit provider may not hold CRB derived information, clause 21V imposes obligations on credit providers to provide assistance to an individual who wishes to correct credit information, CRB derived information, or CP derived information about the individual. If the credit provider holds at least one of these categories of information they have certain correction obligations, and the ability to consult with another credit reporting body or credit provider as required.

To the extent that a credit provider handles any other personal information, the APPs will regulate the handling of that personal information by credit providers that are APP entities.

Subdivision B – Consideration of information privacy

Clause 21B Open and transparent management of credit information etc.

Clause 21B is based on the obligations set out in APP 1, modified to apply specifically to credit providers and their handling of credit information and credit eligibility information. The interaction of this provision with APP 1 is dealt with in subclause (7).

Subclause (1) states the object of the provision.

Subclause (2) imposes a general requirement on credit providers to take reasonable steps to implement practices, procedures and systems in relation to their functions or activities as a credit provider that will ensure compliance with: the requirements of the Division and the registered CR code; and to enable them to deal with inquiries or complaints about their compliance. It is anticipated that credit providers will demonstrate their compliance with this obligation by, for example, developing and maintaining training programs, staff manuals, standard procedures and any other relevant documents that demonstrate awareness of, and compliance with, their obligations under the Division and the registered CR code. In addition, credit providers should be able to demonstrate that their business systems, such as their data management systems, comply with the requirements of the Division or the registered CR code.

Subclause (3) requires credit providers to have a policy dealing with their management of credit information and credit eligibility information. The policy must be clearly expressed and up-to-date.

Subclause (4) provides a list of matters on which the policy must contain information. The list is not exhaustive and the policy can, and should where necessary to satisfy the obligation set out in subclause (3), contain additional information. The purpose of the list is to provide guidance to credit providers on information that the policy must contain which is likely to be directly relevant to individuals and their concerns about the information handling practices of credit providers. It is not intended that the policy set out matters such as detailed operational or administrative procedures or the processes of internal data management systems, nor is it intended that the policy establish technical data handling standards.

Subclause (5) requires credit providers to take reasonable steps to make the policy publicly available. Credit reporting bodies must take reasonable steps to make the policy available free of charge, and must make the policy available in an appropriate form – for example, on the website'.

Subclause (6) ensures that the policy is readily available to the public. While a credit provider may decide to make the policy available on their website, there may be circumstances where a person or body may wish to have the policy in a particular form – for example, in a different digital form that is more accessible for readers with a disability, or as a printed booklet. Following any such request, credit providers must take reasonable steps to provide the person or body with a copy of their policy in the requested form. It is expected that credit providers would not charge for making the policy available in the requested form.

Subclause (7) deals with the interaction of this provision with the APPs. It makes clear that APPs 1.3 and 1.4 (which deal with privacy policies) do not apply to the credit provider in relation to credit information or credit eligibility information. However, the APPs will continue to apply to the credit provider in relation to any other personal information.

Subdivision C – Dealing with credit information

Subdivision C sets out rules for credit providers in relation to credit information. This is the information that credit providers disclose to credit reporting bodies into the credit reporting system. Rules to deal with information that credit providers collect from the credit reporting system are set out in Subdivision D.

Clause 21C Additional notification requirements for the collection of personal information etc.

Clause 21C sets out additional notification requirements for credit providers when they collect personal information that may be disclosed to a credit reporting body (only that personal information which falls within the definition of credit information may be disclosed). Credit providers must notify individuals about certain matters to whom they are likely to disclose information, and credit providers that are APP entities must also notify individuals of certain matters in relation to the credit provider's credit reporting privacy policy. The interaction of this provision with APP 5 is dealt with in subclause (2).

Subclause (1) applies where a credit provider collects personal information about an individual that is likely to be disclosed to a credit reporting body. At or before the time of collection the credit provider must notify the individual of the name and contact details of the credit reporting body (or bodies, if the information may be disclosed to more than one body) and any other matters specified in the registered CR code. Alternatively, rather than notifying the individual, the credit provider must otherwise ensure that the individual is aware of the matters specified. Depending on the circumstances, other approaches may be more appropriate to inform the individual of this information, for example where the credit provider arranges for a third party to notify the individual. Irrespective of the method used, the individual must be informed of these matters and it is expected that the information about the credit reporting body or bodies would subsequently be readily accessible to the individual for their reference. It is intended that the registered CR code would include requirements to inform individuals of how their personal information will be handled in the credit reporting system. This should include providing information that either includes, or allows the individual to readily access, the privacy policies of credit reporting bodies. As required by clause 20B, the privacy policies of credit reporting bodies must include various matters that are of significance to individuals, including information about access, correction and complaints. Other matters may also be addressed in the registered CR code.

Subclause (2) deals with the interaction of this provision with the APPs. The obligations set out in subclause (1) apply in addition to the obligations imposed on a credit provider that is an APP entity by APP 5.

The credit provider must have a credit reporting privacy policy, as required by clause 21B. Subclause (3) sets out matters contained in the credit reporting privacy policy about which the credit provider must notify the individual or otherwise bring to the individual's attention. This specific notification requirement is to be read with the obligations imposed on a credit provider that is an APP entity by APP 5.

Clause 21D Disclosure of credit information to a credit reporting body

Clause 21D controls the flow of credit information into the credit reporting system by regulating the disclosure of credit information by the credit provider to a credit reporting body. As part of this regulation the provision restrict the credit reporting system to Australian participants and to credit provided, or applied for, in Australia.

Subclause (1) establishes a general prohibition on disclosure by a credit provider of credit information about an individual to a credit reporting body. This prohibition operates irrespective of whether or not the credit reporting body carries on a credit reporting business in Australia. This means that disclosure of credit information to a foreign credit reporting body is prohibited. Breach of this provision is subject to a civil penalty of 2000 penalty units.

Subclause (2) provides an exception to the general prohibition in subclause (1) by permitting disclosures by certain credit providers to certain credit reporting bodies. Before any disclosure can occur, the credit provider must be a member of a 'recognised external dispute resolution scheme' and must know, or believe on reasonable grounds, that the individual about whom credit information is to be disclosed is at least 18 years old. Reasonable grounds will depend on the circumstances, but it is expected that satisfying this obligation would generally require the credit provider to have positively verified the individual's age. This requirement is consistent with the policy of not including personal information in the credit reporting system of individuals who are under 18, except in certain defined circumstances (see subclauses (4) and (5) and clause 20C which sets out the circumstances in which a credit reporting body can collect this information). The credit reporting body to which the disclosure is to be made must be an agency or an organisation or small business operator that has an Australian link. The term Australian link is defined by section 5B of the Act. This provision operates to limit the disclosure of credit information to Australian 'credit reporting bodies'. In addition, the credit information that is disclosed must meet the requirements of subclause (3). The note indicates that, even if these conditions are met, clause 21F provides additional limitations on the disclosure of credit information during a ban period (established under clause 20K) where an individual is the victim of fraud, including identity fraud.

Subclause (3) sets out the conditions with which credit information must comply before it can be disclosed to a credit reporting agency under subclause (2). These conditions are based on the restrictions set out in clause 20C that apply to the collection of credit information by credit reporting bodies.

Paragraph (a) states that the credit information must not relate to an act, omission, matter or thing that occurred or existed before the individual turned 18. However, subclause (4) permits identification information about an individual to be disclosed. Clause 20C states that a credit reporting body can only collect identification information where it already holds, or collects at the same time, consumer credit liability information about the individual. In addition, subclause (5) permits consumer credit liability information about an individual under 18 to be disclosed where the credit has not been terminated or otherwise ceased to be in force before the individual turned 18. The issue of whether credit has been terminated or otherwise ceases to be in force will depend on the terms of the consumer credit. Depending on the type of consumer credit, in some circumstances the individual may continue to have access to the credit after repaying the credit. This means that the consumer credit would not be taken as terminated until the individual no longer had access to the credit. Credit providers should clearly indicate to consumers the circumstances in which their credit will be terminated, and whether the consumer must take any action in addition to making the final repayment to terminate the credit. There may be other circumstances in which the credit is terminated – for example, by a serious credit infringement. The registered CR code will provide additional guidance on determining the day on which consumer credit is terminated and the other circumstances in which the consumer credit ceases to be in force

Paragraph (b) says that any credit information that relates to consumer or commercial credit must relate to credit that is or has been provided, or applied for, in Australia. Information

about the foreign credit activities of individuals cannot be included in the credit reporting system.

Paragraph (c) establishes certain restrictions around credit information that is repayment history information. It can only be disclosed if: the credit provider is a 'licensee' (and hence subject to responsible lending obligations under the National Consumer Credit Protection Act); the consumer credit liability information to which the repayment history information relates must also be, or have been previously, disclosed to the credit reporting body; and the credit provider must comply with any additional requirements in relation to the disclosure of the information prescribed by regulations. It is expected that regulations will deal with matters such as how to determine whether a payment is a monthly payment and other relevant matters.

Paragraph (d) permits disclosure of credit information that is default information only where the credit provider has given the individual written notice stating the intention to disclose the default information to a credit reporting body, and a reasonable period has passed since the giving of the notice. The purpose of this additional notification requirement is to ensure that credit providers have done everything reasonable to make individuals aware of the proposed default listing. It would also provide individuals with one final opportunity to make overdue payments. The reasonable period that must elapse between the giving of the notice and disclosing the default information to a credit reporting body will depend on the circumstances, and it is expected that additional guidance around the appropriate timeframes will be provided in the registered CR code.

Subclause (6) requires credit providers to make a written note of any disclosure of credit information under this provision. This is consistent with the policy of requiring credit reporting bodies to make written notes of disclosures. Certain other Acts set out circumstances in which credit reporting bodies must not make notes (see the note to clause 20E). A similar note has not been inserted in this provision because there are no Acts which currently set out circumstances in which credit providers must not make a written note of disclosures. If any such provisions were enacted in another Act in the future, then that other Act would operate to limit the making of written notes by credit providers. The purpose of requiring notes is to provide a record of all disclosures. To be an effective record, the written note should identify the date of the disclosure, the entity to which the credit reporting information was disclosed, the type of disclosure (including the specific provision under which the disclosure was authorised), the type of credit information that was disclosed (where this is not clear from the type of disclosure), and any other relevant information. Written notes should be sufficiently associated with the credit reporting information of the relevant individual to ensure that individuals are able to obtain access to all written notes relating to their credit information. Written notes do not themselves fall within the definition of credit information or credit reporting information. However, as written notes would be personal information about an individual, a credit provider that is an APP entity will be subject to the general obligations set out in the APPs in relation to the written notes of disclosures. A breach of this provision attracts a civil penalty of 500 penalty units.

Subclause (7) deals with the interaction of this provision with the APPs. It makes clear that APPs 6 and 8 (which deal with use and disclosure and cross-border disclosures) do not apply to a credit provider that is an APP entity in relation to the disclosure of credit information to a credit reporting body. However, these APPs will continue to apply to a credit provider that is an APP entity in relation to any other personal information the credit provider may hold (except for credit eligibility information, which is dealt with in Subdivision C). In this regard, it is important to note that any personal information held by a credit provider that is

an APP entity will always be subject to the protections available under the Privacy Act. In general terms, the APPs will apply to the information, unless specific kinds of personal information are subject to different rules set out in the credit reporting provisions.

Clause 21E Payment information must be disclosed to a credit reporting body

Clause 21E requires credit providers to disclose certain information about the payment of overdue credit obligations. The purpose of this provision is to ensure that a person who subsequently makes an overdue payment that has been listed as a default has that payment recorded along with the relevant default as part of the individual's credit information. The payment information (which is a defined term) may be disclosed to credit providers (as permitted by Division 2) and will be available to assist credit providers to make decisions about an individual's credit worthiness.

Where a credit provider has disclosed default information about an individual to a credit reporting body, and after the default information was disclosed the amount of the overdue payment was paid, the credit provider must disclose that payment information to the credit reporting body within a reasonable period after the payment is made. It is expected that the registered CR code will provide guidance to assist in determining what is a reasonable period. Failure to comply with this provision is subject to a civil penalty of 500 penalty units.

Clause 21F Limitation on the disclosure of credit information during a ban period

Clause 21F is linked with provisions in Division 2 to provide a thorough response to identity fraud issues. Clause 20K establishes a mechanism for individuals to deal with potential fraud, including identity fraud, by controlling the disclosure of their credit reporting information in certain circumstances. Clause 20Y provides for the destruction of credit reporting information by the credit reporting body in cases of fraud.

Clause 21F limits the disclosure by credit providers of credit information to credit reporting bodies during a ban period. If a credit provider is unable to obtain access to an individual's credit reporting information to assess an application for credit due to a ban period but proceeds to provide credit to a person purporting to be the individual, the credit provider cannot list any of the information about that credit as part of the individual's credit information. This is intended to ensure that credit providers take reasonable steps to identify a person during a ban period.

Subclause (1) sets out the circumstances in which this provision will operate. The provision applies if: a credit reporting body holds information about an individual; a credit provider requests disclosure of the individual's information to assess an application for consumer credit made by the individual or someone purporting to be the individual; the information cannot be disclosed because a ban period is in place; and during the ban period, consumer credit is provided to the individual or the person purporting to be the individual.

A credit reporting body is not prohibited from telling a credit provider whether or not it holds credit reporting information about an individual, nor is it prohibited from telling a credit provider that a ban period is in place in relation to an individual. The purpose of these provisions is not to prevent a credit provider from knowing about the ban period, but to prevent access to the individual's credit reporting information without the express consent of the individual.

If subclause (1) is satisfied, subclause (2) provides that the credit provider must not disclose to a credit reporting body any credit information that relates to consumer credit. Breach of this prohibition is subject to a civil penalty of 2000 penalty units.

Subclause (3) states that the prohibition in subclause (2) does not apply if the credit provider has taken such steps as are reasonable in the circumstances to verify the identity of the individual to whom the provider intends to provide the credit. The reasonable steps will depend on the circumstances in each case.

It is expected that further practical details around the operation of the provisions dealing with ban periods in cases of fraud would be covered in the registered CR code. Matters that may be covered include: notifying the individual of the effect of the ban period and the circumstances in which the individual should be notified that the ban period is ending; the extension of the ban period; notification of credit providers of the ban period; and other relevant matters.

Subdivision D – Dealing with credit eligibility information etc.

Subdivision C sets out rules for credit providers in relation to credit eligibility information. This category of information incorporates the credit reporting information that credit providers collect from the credit reporting system as well as any CP derived information. Rules to deal with information that credit providers disclose to credit reporting bodies into the credit reporting system are set out in Subdivision B.

This Subdivision contains rules on uses and disclosures of credit eligibility information by credit providers, including rules that provide for disclosures to specific kinds of recipients. This Subdivision also contains a rule providing for notification of the individual following a refusal of an application for consumer credit based wholly or partly on credit eligibility information about certain persons.

Clause 21G Use or disclosure of credit eligibility information

Clause 21G sets out the general rules for the use or disclosure of credit eligibility information by credit providers. This provision is based on the obligations and structure of APP 6, but has been significantly modified to apply specifically to credit providers and credit eligibility information. Clause 21G is similar in structure to clause 20E, which deals with use and disclosure by credit reporting bodies of credit reporting information.

Subclause (1) establishes a general prohibition on the use or disclosure of credit eligibility information about an individual by a credit provider. Breach of this prohibition is subject to a civil penalty of 2,000 penalty units. Subclauses (2) and (3) provide exceptions for this general prohibition.

Subclause (2) sets out the permitted uses, which are exceptions to the prohibition on using credit eligibility information in subclause (1). Paragraph (2)(a) provides that a credit provider is permitted to use credit eligibility information if the use is for a 'consumer credit related purpose' in relation to the individual. 'Consumer credit related purpose' is a defined term and means that the use must be for the purpose of assessing an application for consumer credit made by the individual, or collecting payments that are overdue in relation to consumer credit provided to the individual.

Paragraph (2)(b) provides that a 'permitted CP use' in relation to an individual is allowed, and the permitted CP uses are set out in clause 21H. Paragraph (2)(c) permits the use of credit eligibility information in relation to serious credit infringements. The provider must believe on reasonable grounds that the individual has committed a serious credit infringement and the use of the information must be in connection with the infringement. For example, the use may be to try to obtain up-dated identification information to check whether the individual has moved to a new address to allow the provider to try to contact the individual again.

Paragraphs (2)(d) and (e) also permit a credit provider to use credit eligibility information if the use is required or authorised by or under Australian law or a court or tribunal order, or the use is prescribed in the regulations. The regulation-making power provides a means to permit any currently unforeseen but necessary uses that may arise in the future. Additional uses will be permitted where the use can be shown to be in the public interest as well as being for the benefit of the individuals whose credit eligibility information would be used. Appropriate public consultation with all relevant stakeholders would be undertaken when considering whether regulations prescribing any additional uses should be prepared.

Unlike APP 6, no secondary uses of credit eligibility information by a credit provider are permitted. Only those uses expressly provided in subclause (2) and clause 21H are permitted.

Subclause (3) sets out the permitted disclosures, which are exceptions to the prohibition on disclosing credit eligibility information in subclause (1). Paragraph (3)(a) provides that a credit provider does not breach this provision if the disclosure is a 'permitted CP disclosure' in relation to the individual. 'Permitted CP disclosure' has the meaning given by clauses 21J to 21N, which set out a range of circumstances for permitted disclosures.

The remaining paragraphs of subclause (3) set out specific permitted disclosures. Paragraph (3)(b) permits disclosures of credit eligibility information to a related body corporate of the credit provider and the related body corporate must have an 'Australian link'. Paragraph (3)(c) permits disclosures to a person who manages credit provided by the credit provider. The credit manager must not be acting as an agent of the credit provider and must have an 'Australian link' to ensure that the credit manager is not a foreign entity. 'Agents of credit providers' is a concept defined in clause 6H, which treats agents as being the credit provider in the circumstances defined. A credit manager is intended to be someone who is not acting as the credit provider's agent but instead provides a service to the credit provider to manage credit accounts. The kinds of services that may be performed by a credit manager will depend on the relationship with the credit provider and decisions made by the credit provider about how it will manage its credit accounts. Recognizing that circumstances will vary, the term credit manager has not been defined.

Paragraph (3)(d) permits disclosure of credit eligibility information to another credit provider that has an 'Australian link' and to enforcement bodies in relation to 'serious credit infringements'. Before making the disclosure the credit provider must believe on reasonable grounds that the individual has committed a 'serious credit infringement'. This provision will assist enforcement bodies in the investigation of alleged serious credit infringements. It will also permit credit providers to alert other providers that they reasonably believe the individual has committed a serious credit infringement.

Paragraph (3)(e) permits disclosures to external dispute resolution schemes that have been recognised by the Commissioner and a credit provider or credit reporting body is a member of the scheme. This provision is intended to ensure that external dispute resolution schemes can access relevant credit eligibility information, where appropriate, to assist in the resolution of complaints made by individuals about their personal information in the credit reporting system.

Paragraphs (3)(f) and (g) also permit a credit provider to disclose credit eligibility information if the disclosure is required or authorised by or under Australian law or a court or tribunal order, or the disclosure is prescribed in the regulations. The regulation-making power provides a means to permit any currently unforeseen but necessary disclosures that may arise in the future. As stated above in relation to the regulation-making power for uses of credit eligibility information, this power would be exercised where the disclosure is in the

public interest, for the benefit of the individual, and following appropriate public consultation.

Subclauses (4) and (5) impose additional limitations where the proposed disclosure is credit eligibility information that includes, or was derived from, repayment history information. Subclause (4) prohibits the disclosure of such information. The civil penalty for breach of subclause (4) is 2,000 penalty units. Subclause (5) provides for exceptions to this prohibition in specified circumstances. Paragraph (5)(a) provides that this information can be disclosed if the recipient is another credit provider who is a 'licensee'. This is intended to ensure that repayment history information, or credit eligibility information that is derived from repayment history information, can only be disclosed to credit providers who are subject to responsible lending obligations under the National Consumer Credit Protection Act. This restriction extends to credit eligibility information that was derived from repayment history information because it is considered appropriate that credit providers who cannot access repayment history information should not be able to indirectly obtain the benefit of that information through the possibility that credit providers could provide credit eligibility information that incorporates repayment history information in another form. Paragraph (5)(b) provides an exception where the information is disclosed under clause 21L, which permits the disclosure of credit eligibility information to mortgage insurers in specified circumstances. As mortgage insurers are underwriting the credit risk taken on by the credit provider in providing consumer credit, it is important that the mortgage insurers have access to the same information available to the credit provider to whom they are offering insurance. Where this information includes repayment history information, a credit provider can disclose this information to the mortgage insurer for the mortgage insurance purpose as specified in clause 21L. A mortgage insurer is prohibited from making any further disclosure of that information by clause 22C (except where that disclosure may be required or authorised by or under an Australian law or court or tribunal order). Paragraph (5)(c) permits disclosure of the information to an enforcement body for the purposes of paragraph (3)(d) (where the disclosure is related to a serious credit infringement). Paragraph (5)(d) permits disclosure for the purposes of paragraph (3)(e) (to a recognised external dispute resolution scheme) and for the purposes of paragraph (3)(f) (where the disclosure is required or authorised by or under an Australian law or a court or tribunal order).

Subclause (6) requires credit reporting bodies to make a written note of any use or disclosure of credit eligibility information under this provision. Because subclause (2) includes permitted CP uses under clause 21H and subclause (3) includes permitted CP disclosures under clauses 21J to 21N, this means that written notes will need to be made of all these uses and disclosures. The purpose of requiring notes is to provide a record of all uses and disclosures of credit eligibility information. To be an effective record, the written note should identify the date of the use or disclosure, the type of use or disclosure (including the specific provision under which the disclosure is authorised), the entity to which the credit eligibility information was disclosed, the type of credit eligibility information that was disclosed (where this is not clear from the type of disclosure), and any other relevant information (for example, that an individual's express consent to a disclosure under clause 21J was not in writing because of the circumstances set out in subclause 21J(2)). In relation to identifying the type of credit eligibility information that was disclosed, a reader of the note should be able to determine whether all credit eligibility information relating to the individual was disclosed, and if not, what types of credit eligibility information were disclosed (for example, repayment history information). Written notes should be sufficiently associated with the credit eligibility information of the relevant individual to ensure that individuals are able to obtain access to all written notes relating to their credit eligibility information.

Written notes do not themselves fall within the definition of credit information or credit eligibility information. However, as written notes would be personal information about an individual, a credit provider that is an APP entity will be subject to the general obligations set out in the APPs in relation to the written notes of uses and disclosures. A breach of this provision attracts a civil penalty of 500 penalty units.

Subclauses (7) and (8) both deal with the interaction of this provision with the APPs. Subclause (7) makes clear that APPs 6 and 8 (which deal with use and disclosure and cross-border disclosures) do not apply to a credit provider that is an APP entity in relation to credit eligibility information. Subclause (8) provides that, where the credit eligibility information is a government related identifier of the individual (for example, a driver's licence number), APP 9.2 (which deals with the use or disclosure of such identifiers) does not apply. However, these APPs will continue to apply to the credit provider in relation to any other personal information the credit provider may hold (except for credit information, which is dealt with above in Subdivision B). In this regard, it is important to note that any personal information held by a credit provider that is an APP entity will always be subject to the protections available under the Privacy Act. In general terms, the APPs will apply to the information if the credit provider is an APP entity, unless specific kinds of personal information are subject to different rules set out in the credit reporting provisions.

Clause 21H Permitted CP uses in relation to individuals

This provision sets out the circumstances in which a use of credit eligibility information by a credit provider will be a 'permitted CP use' authorised by paragraph 135(2)(b). This provision refers to the permitted disclosures of credit reporting information by a credit reporting body pursuant to the table in subclause 20F(1). It is important to remember the data flows in the credit reporting system and the terms used to describe that data at different points in the system. Credit reporting information about an individual disclosed by a credit reporting body will become credit eligibility information when the recipient credit provider collects it. 'Credit eligibility information' is held by credit providers and is defined as credit reporting information or any 'CP derived information' about the individual.

The provision states that a use of credit eligibility information is permitted where the relevant credit reporting information was disclosed to the credit provider under the provision specified in column 1 of the table (that is, a provision from the table in subclause 20F(1) that permitted a credit reporting body to disclose the information) for the specified purpose. In these circumstances, the use set out in column 2 of the table is permitted by the credit provider. The table lists six permitted CP uses.

Item 1 of the table provides that a disclosure of credit reporting information for the purpose of assessing an application for consumer credit made by the individual to the credit provider can be used for a 'securitisation related purpose' of the credit provider, or the information can be used for the internal management purposes of the provider that are directly related to the provision or management of consumer credit by the provider. Essentially, the information that has been disclosed under this item can already be used under paragraph 21G(2)(a) for a 'consumer credit related purpose', so this item permits these two additional uses to be made of this information. While item 6 also deals with uses for securitisation related purposes, item 6 applies to a different recipient. In the case of item 1, the recipient is the credit provider who has assessed an application for credit and that credit provider is now engaging in securitisation activities. Item 6 of the table, discussed further below, applies to securitisation entities that are, for the purposes of that activity, defined as a credit provider. The other permitted purpose for which the information may be used under item 1 is internal

management purposes of the credit provider that are directly related to the provision or management of consumer credit by the provider. This will allow the provider to use the information for the purposes of deriving 'CP derived information' about the individual, to manage its relationship with the individual as well as to manage its credit business as a whole. This would permit the credit provider to use the information for data management purposes, for example, or other activities necessary to run the consumer credit business of the provider.

Item 2 of the table permits information that has been disclosed to the credit provider for a particular 'commercial credit related purpose' to be used for that purpose. This means the information can only be used for the purpose of assessing an application for commercial credit or to collect overdue payments in relation to commercial credit provided to the individual. The table in subclause 20F(1) requires that the individual must have already expressly consented to the disclosure by the credit reporting body of the credit reporting information to the credit provider for this commercial credit purpose. The requirement for express consent ensures that the individual is aware that their credit information will be used for a non-consumer credit purpose.

Item 3 of the table also refers to disclosures of credit reporting information made for a commercial credit purpose, but in this case the disclosure must be made for the specific purpose of assessing an application for commercial credit made by the individual to the provider, and the permitted use is not for assessing that application (which is dealt with in item 2 above) but instead is for the internal management purposes of the provider that are directly related to the provision or management of commercial credit by the provider. This means that the information can be used by the credit provider for deriving information about the individual in relation to their commercial credit (similar to the category of information called 'CP derived information', but that category refers to consumer credit). In this context derived information may mean a credit score in relation to the individual's commercial credit worthiness. Item 3 is limited to credit reporting information disclosed for the purposes of assessing the application and does not permit the use of information disclosed for the purpose of collecting overdue payments for internal management purposes in relation to commercial credit. This limitation ensures consistency with the permitted uses in the consumer credit context. Credit eligibility information which was disclosed for the purpose of assessing an application for commercial credit made by a person to the credit provider could also be used for other internal management purposes, such as data management. Once again, the table in subclause 20F(1) requires that the individual must have already expressly consented to the disclosure by the credit reporting body of the credit reporting information to the credit provider.

Item 4 of the table provides that information that has been disclosed to the credit provider for a 'credit guarantee purpose' of the provider in relation to the individual can only (if directly related to the provision or management of commercial credit by the provider) be used for that 'credit guarantee purpose' or for the internal management purposes of the provider directly related to the provision or management of any credit by the provider. This information can only be disclosed by the credit reporting body once the individual has expressly consented, in writing, to the use of the information for the credit guarantee purpose. 'Credit guarantee purpose' is a defined term, and means the purpose of assessing whether to accept the individual as a guarantor in relation to credit provided to, or applied for by, another person. In this context, it is the individual who is proposing to be the guarantor whose information is being disclosed. This information can be used for internal management purposes directly related to any credit provided by the provider – both commercial credit and consumer credit.

Item 5 of the table permits information that has been disclosed to a current credit provider of an individual (that is, a credit provider who provides consumer credit to the individual that has not been terminated or otherwise ceased to be in force) to be used for the purpose of assisting the individual to avoid defaulting on his or her consumer credit obligations to the provider. When read with item 5 in the table at subclause 20F(1) this provision has the effect of limiting the use of any information disclosed to assisting the individual to avoid defaulting on the individual's consumer credit obligations to that credit provider. It would not be consistent with the purpose of the credit reporting system for the provider to obtain regular disclosures from the credit reporting body simply to monitor or check an individual's overall credit worthiness or behaviour

Item 6 of the table permits information that has been disclosed to a credit provider for a securitisation related purpose of the credit provider in relation to the individual to be used for that particular securitisation purpose. A 'securitisation related purpose' refers to assessing the risk of purchasing, by means of a securitisation arrangement, credit that has been provided to the individual or to a person to whom the individual is or proposes to be a guarantor. The definition of the term also refers to assessing the risk in undertaking credit enhancement in relation to credit that has been provided to an individual (or a person to whom the individual is or may be a guarantor) through a securitisation arrangement.

Clause 21J Permitted CP disclosures between credit providers

This provision sets out the circumstances in which a disclosure of credit eligibility information between credit providers will be a 'permitted CP disclosure' authorised by paragraph 21G(3)(a). Four circumstances are identified where a credit provider can disclose information to another credit provider – where the individual consents; where the disclosure is to the agent of a credit provider; in relation to certain securitisation arrangements; and where the disclosure is in relation to mortgage credit secured by the same property – and these circumstances are subject to the specific requirements detailed in this provision. The credit provider who collects credit eligibility information will be subject to the any conditions set out in this provision in relation to that disclosure as well as any applicable general conditions imposed upon credit providers in relation to the use of credit eligibility information as set out in subclause 21G(2). Similarly, both the disclosing and the using credit providers will be required to make written notes of their disclosures and uses consistent with the obligation imposed by subclause 21G(6).

Subclause (1) permits a disclosure of credit eligibility information in relation to an individual to another credit provider where the disclosure is for a particular purpose, the credit provider that is the recipient of the information has an Australian link, and the individual has expressly consented to the disclosure of the information to the recipient for the particular purpose. The requirement that the recipient have an Australian link is consistent with the restriction of the credit reporting system to Australian entities and ensures that the credit provider is not a foreign entity. The particular purpose of the disclosure will be limited by the permitted uses of a credit provider set out in subclause 21G(2). The requirement for express consent is subject to the rules set out in subclause (2). The express consent of the individual to the disclosure for the particular purpose must be given in writing. The only exception to the writing requirement is where the disclosure is for the purpose of assessing an application for consumer or commercial credit made by the individual and the individual did not make the application for credit in writing. This provision does <u>not</u> mean that the individual does not need to provide consent where the application was not in writing. Instead, it means that where the individual's application was not in writing the individual's express consent also does not need to be in writing. However, the individual must still provide express consent to

the disclosure. The consent of the individual (whether in writing or not) must be given to the credit provider who is to disclose the information or to the credit provider who will be the recipient of the information. It is not necessary for the consent to be given to both credit providers. Circumstances where the disclosing credit provider would be given the consent may include where the consent is not in writing. This would enable the disclosing credit provider to confirm that the individual has provided express consent to the disclosure for the particular purpose.

Subclause (1) would not affect any practices credit providers may have in place to share other personal information, with appropriate consent from the individual, outside the credit reporting system where such practices are consistent with the obligations imposed by the APPs on credit providers in their capacity as APP entities. However, the information sharing practices must comply with the requirements of this provision to the extent that any such information sharing practices include dealing with credit eligibility information (which, by operation of the definitions, includes 'credit information' and' CP derived information').

Subclause (3) permits a credit provider that is acting as an agent to disclose credit eligibility information about an individual back to the credit provider that is the principal in the agency relationship. The credit provider making the disclosure under this provision must be acting as an agent of another credit provider that has an Australian link. The requirement that the credit provider have an Australian link is consistent with the restriction of the credit reporting system to Australian entities and ensures that the credit provider is not a foreign entity. The credit provider making the disclosure under this provision must be a credit provider in the terms set out in subclause 6H(1), which sets out the rules for determining whether an organization or small business operator is an agent of a credit provider. The final element in this provision that must be satisfied is that the credit provider (that is, the agent) must be making the disclosure in their capacity as an agent of the principal credit provider. This provision recognises that there are different organizational structures in the credit industry and in some instances an entity is in fact a credit provider only because it is acting as the agent of a credit provider. In such situations, the agent must be able to disclose information to the principal in the agent/principal relationship. Such disclosures would otherwise be prohibited without this provision.

Subclause (4) permits a credit provider that is acting as a securitisation entity to disclose credit eligibility information about an individual back to the original credit provider that provided the credit to which the securitisation arrangements relate. This provision permits certain disclosures to occur that are necessary due to securitisation relationships between entities and credit providers. Such disclosures would otherwise be prohibited without this provision. The credit provider making the disclosure must be a credit provider under subclause 6J(1), which deals with securitisation entities that are taken to be credit providers for the purposes of performing tasks necessary for a securitisation arrangement. The original credit provider of the credit (or application for credit, as the case may be) to which the securitisation relates must have an Australian link. The requirement that the credit provider have an Australian link is consistent with the restriction of the credit reporting system to Australian entities and ensures that the credit provider is not a foreign entity. The original credit provider cannot be a credit provider by the operation of subclause 6J(1). This provision is intended to break the chain of relationships between entities. An entity that is only a credit provider because it is performing securitisation related tasks cannot then form a securitisation relationship with another entity and then claim that it is the original credit provider. If any such relationships are entered, they will not satisfy the requirements for this provision to allow the disclosure of credit eligibility information. The credit eligibility information that is the subject of the disclosure must be disclosed to the original credit

provider or another credit provider that subclause 6J(1) defines as a credit provider in relation to that credit (and in this case, the other credit provider must have an Australian link. The last requirement in this rule that must be satisfied for the disclosure to be permitted is that the disclosure of the information must be reasonably necessary for a securitisation purpose as set out in subparagraphs (4)(e)(i) and (ii). The end result of this provision is that it permits disclosures between entities that are involved in a securitisation arrangement, as that relationship is defined in subclause 6J(1).

Subclause (5) permits a credit provider to disclose credit eligibility information about an individual to another credit provider that has provided mortgage credit to the individual secured by the same real property. However, the disclosure is only permitted where the information relates to overdue payments. As with the other provisions, the disclosure can only be to another credit provider that has an Australian link. The requirement that the credit provider have an Australian link is consistent with the restriction of the credit reporting system to Australian entities and ensures that the credit provider is not a foreign entity. Both credit providers must have provided mortgage credit in relation to which the same real property forms all or part of the security. The individual must be at least 60 days overdue in making a payment in relation to the mortgage credit provided by either provider. The final element of this rule that must be satisfied is that the information must be disclosed for the purpose of either provider deciding what action to take in relation to the overdue payment.

Clause 21K Permitted CP disclosures relating to guarantees etc.

This provision sets out the circumstances in which a disclosure of credit eligibility information relating to guarantees will be a 'permitted CP disclosure' authorised by paragraph 21G(3)(a). This provision deals with disclosures of information about an individual in two situations: where the disclosure is to a person who is considering whether to offer to act as a guarantor for the person; and where the disclosure is to a person who is already a guarantor of the credit in relation to that individual for certain purposes in relation to that guarantee.

Subclauses (1) and (2) deal with disclosures to a person who is considering whether to act as a guarantor for an individual. Subclause (1) provides that a disclosure of credit eligibility information about an individual by a credit provider is a permitted disclosure if the credit provider has provided credit to the individual or the individual has applied to the provider for credit. The disclosure must be to a person for the purpose of that person considering whether to offer to act as a guarantor in relation to credit or to offer property as security for the credit. The person (that is, the potential guarantor) must have an Australian link. The requirement that the person have an Australian link is consistent with the restriction of the credit reporting system to Australia. In addition, the individual whose information is to be disclosed must expressly consent to the disclosure to the person for that purpose. Subclause (2) provides that the express consent must be given in writing unless the application for the credit that has been provided was not made in writing, or the application for the credit that is being considered was not made in writing. In these circumstances, express consent is still required but the consent does not need to be in writing. Disclosures in the circumstances prescribed are intended to provide the prospective guarantor with sufficient information to make an informed decision about the individual's credit worthiness and whether to provide a guarantee for the individual.

Subclauses (3) and (4) deal with disclosures to an existing guarantor where the individual either: expressly consents to the disclosure; or the disclosure is for a purpose related to the enforcement, or proposed enforcement, of the guarantee. Subclause (3) requires the disclosure to be to a person who is a guarantor in relation to credit provided by the provider

to the individual, or who has provided property as security for the credit. The person must have an Australian link, consistent with the restriction of the credit reporting system to Australia. In addition, the individual must either expressly consent to the disclosure, or (where the person is a guarantor in relation to the credit) the disclosure is for a purpose related to the enforcement, or proposed enforcement, of the guarantee. Subclause (4) provides that the express consent must be given in writing unless the application for the credit that was provided was not made in writing. In these circumstances, express consent is still required but the consent does not need to be in writing. Express consent is not required where the disclosure is related to the enforcement or proposed enforcement of the guarantee.

Clause 21L Permitted CP disclosures to mortgage insurers

This provision sets out the circumstances in which a disclosure of credit eligibility information to mortgage insurers will be a 'permitted CP disclosure' authorised by paragraph 21G(3)(a). Mortgage insurers require access to certain credit eligibility information to assess their risk in underwriting credit, and for this purpose it is also necessary for the mortgage insurer to have access to information that allows the mortgage insurer to assess the risk of the credit provider that is providing the mortgage credit, and the risk of individuals defaulting on the credit or being unable to meet their commitments under a guarantee.

Clause 21L permits a disclosure by a credit provider of credit eligibility information about an individual if it is to a mortgage insurer that has an Australian link, consistent with the restriction of the credit reporting system to Australia. The disclosure must be for a 'mortgage insurance purpose' of the insurer in relation to the individual or for any purpose arising under a contract for mortgage insurance that has been entered into between the credit provider and the mortgage insurer. A 'mortgage insurance purpose' is defined and, in summary, means for the purpose of assessing: whether to provide insurance to a credit provider in relation to mortgage credit; the risk of an individual defaulting on mortgage credit in relation to which insurance has been provided to the provider; or the risk of the individual being unable to meet a liability under a guarantee provided in relation to the mortgage credit of another person.

Mortgage insurers are subject to further obligations in Division 4 in relation to their privacy policies (clause 22A), notification requirements (clause 22B), and any further use and disclosure of information they have collected (clause 22C).

Clause 21M Permitted CP disclosures to debt collectors

This provision sets out the circumstances in which a disclosure of credit eligibility information to debt collectors will be a 'permitted CP disclosure' authorised by paragraph 21G(3)(a). Disclosures to debt collectors are permitted only in limited circumstances and the information that can be disclosed is also restricted.

Subclause (1) provides that the disclosure must be to a debt collector – that is, a person or body that carries on a business or undertaking that involves the collection of debts on behalf of others. That person or body must have an Australian link, consistent with the restriction of the credit reporting system to Australia. The disclosure of the information must be for a purpose directly related to the actual collection of payments that are overdue in relation to consumer credit provided by the provider to the individual, or commercial credit provided by the provider to a person. However, the kinds of information that can be disclosed are restricted to those set out in subclause (2).

Subclause (2) restricts the kinds of credit eligibility information about an individual that can be disclosed to information that is: 'identification information'; 'court proceedings information'; 'personal insolvency information'; or, where the disclosure is in relation to overdue consumer credit payments, 'default information'. However, default information can

only be disclosed if the credit provider does not hold, or has not previously held, payment information about the individual that relates to that overdue payment.

Debt collectors that are APP entities must comply with the obligations set out in the APPs in relation to the handling of any information disclosed under this provision. Debt collectors that are a small business for the purposes of section 6D of the Act may not be subject to the APPs, depending on the circumstances of that debt collector and the conditions set out in section 6D.

Clause 21N Permitted CP disclosures to other recipients

This provision sets out the circumstances in which a disclosure of credit eligibility information to other recipients will be a 'permitted CP disclosure' authorised by paragraph 21G(3)(a). The other recipients to which disclosures may be permitted are mortgage credit assistance schemes and certain entities in relation to the assignment of debts owed to the credit provider.

Subclause (1) permits the disclosure of credit eligibility information about an individual to a State or Territory authority whose functions or responsibilities include either giving assistance (directly or indirectly) that facilitates the provision of mortgage credit to individuals, or managing or supervising schemes or arrangements that provide such assistance. The information must be disclosed for the purpose of enabling the authority to determine the extent of the assistance, if any, to give in relation to the provision of mortgage credit to the individual, or for the purpose of managing or supervising a scheme or arrangement that provides the assistance. The subsequent handling of the information by the State or Territory authority will be subject to the laws of that State or Territory.

Subclauses (2) and (3) deal with disclosures to certain entities in relation to the assignment of debts owed to the credit provider. Subclause (2) sets out the rules to identify the recipients of the information. The recipient must be one or more of: an entity; a professional legal adviser of the entity; or a professional financial advisor of the entity. Any recipient of the information must have an Australian link, consistent with the restriction of the credit reporting system to Australia, and subclause (3) must also apply to the information. Subclause (3) sets out the rules in relation to the proposed uses of the information. The credit eligibility information can only be disclosed if the recipient proposes to use the information in the process of the entity considering whether to: accept an assignment of a debt owed to the credit provider; accept a debt owed to the provider as security for credit provided to the provider; or purchase an interest in the provider or a related body corporate of the provider. Alternatively, the recipient may propose to use the information in connection with exercising rights arising from the acceptance of such an assignment or debt, or the purchase of such an interest.

The recipients of the information under subparagraph (2)(a) are subject to further obligations in Division 4 in relation to their privacy policies (clause 22A), notification requirements (clause 22B), and any further use and disclosure of information they have collected (clause 22F).

Clause 21P Notification of a refusal of an application for consumer credit

This provision sets out the circumstances in which a credit provider must notify an individual of a refusal of an application for consumer credit where the refusal is based in whole or in part on credit eligibility information about certain persons. The purpose of this provision is to increase the transparency of the credit reporting system to individuals by ensuring that they are aware of the role their credit eligibility information has played in the provider's decisions about their application for consumer credit. This also provides an opportunity for the

individual to obtain access to their credit reporting information held by a credit reporting body and which was disclosed to the credit provider and, if necessary, to take steps to correct that information. Accordingly, the information that must be provided to the individual includes information about the relevant credit reporting body and any other matters (such as information about access and correction rights or complaints procedures) that are set out in the registered CR code.

Subclause (1) sets out a number of preliminary rules for the application of this provision. A credit provider must have refused an application for consumer credit made in Australia by an individual or made jointly with one or more other applicants. The refusal of credit must be based wholly or partly on credit eligibility information about one or more of: the individual; a proposed guarantor; or one of the other applicants, if it is a joint application. In addition, a credit reporting body must have disclosed the relevant credit reporting information to the provider for the purposes of assessing the application.

The links between the different categories of information in the credit reporting system are relevant again here. While the refusal must be based on credit eligibility information held by the credit provider, this category of information includes credit reporting information supplied by a credit reporting body. The credit reporting information is relevant because even if the refusal is directly based on the CP derived information contained in the credit eligibility information – that is, for example, the credit provider's own credit scoring processes that reflect the provider's own credit risk parameters – it is also the case that the credit reporting information is likely to have influenced the outcome of that scoring process. In many cases the individual's best option to understand and improve their credit worthiness is to examine and understand their credit reporting information held by the credit reporting body.

This provision will not only operate where a refusal is based wholly on the credit eligibility information, but also where the refusal is based partly on such information. It is recognised that there may be many factors relevant to an assessment by a credit provider of an individual's credit worthiness, including the credit provider's own risk parameters. However, the complexity of the credit reporting system and the connections between information within the system means that it would not be realistic to limit the notification requirement to situations in which an individual's credit eligibility information was wholly responsible for the refusal of an application for credit. There may be situations where an individual will be refused credit wholly because of their credit eligibility information - for example, a default, a personal insolvency agreement, or because of the debt exposure of the individual apparent from the number, type and maximum limit of existing types of credit held by the individual. However, it would not increase the transparency of the credit reporting system and reveal the significant role played by an individual's credit eligibility information in assessing applications for credit if notification was only required where the decision was wholly based on such matters. It is important that notification obligations also apply in situations in which a decision to refuse an application for credit is partly based on an individual's credit eligibility information. This will make the individual aware of the role of their credit eligibility information in the process of assessing their application for credit.

Subclause (2) deals with the notification obligations of the credit provider. The credit provider must, within a reasonable period after refusing the application based wholly or partly on the relevant credit eligibility information, give the individual a written notice. The written notice must state that the application has been refused, state that the refusal is based wholly or partly on credit eligibility information about the individual, a proposed guarantor, or a joint applicant (as appropriate), and, if the information is about the individual, the name

and contact details of the credit reporting body that disclosed the relevant credit reporting information, along with any other matters specified in the registered CR code.

It is expected that the registered CR code will set out additional matters that must be included in the notification provided to the individual. Such matters should include obligations to notify the individual about which elements of the individual's credit eligibility information may have led to the refusal of credit, as well as appropriate access, correction and complaint information. Recognising that a refusal of credit may occur at different stages of the application process, the registered CR code may provide guidance on how the relevant elements are described and any additional information provided to the individual about the refusal. The registered CR code may also set out other relevant matters.

Subdivision E – Integrity of credit information and credit eligibility information

Clause 21Q Quality of credit eligibility information

This provision is based on the obligations set out in APP 10, modified, and with additional provisions, to apply specifically to credit providers. This provision mirrors the obligations imposed by clause 20N upon credit reporting bodies in relation to the quality of credit reporting information.

Subclause (1) provides that a credit provider must take such steps, if any, as are reasonable in the circumstances to ensure that the credit eligibility information the provider collects is accurate, up-to-date and complete. Subclause (2) applies to the use or disclosure of credit eligibility information and includes an additional requirement of relevance. The credit provider must take such steps, if any, as are reasonable in the circumstances to ensure that the credit eligibility information the provider uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant. The additional requirement of relevance means that the actual purpose of the use or disclosure must be considered. These provisions must be read in conjunction with the other provisions in this Division. Other provisions impose various restrictions on the collection, use and disclosure of some or all types of credit eligibility information. The qualification 'if any' used in this provision is also used in APP 10 and recognises that whether or not steps are required will depend upon the circumstances. In addition, these provisions do not require credit reporting bodies and credit providers to enter agreements to ensure that all available information is disclosed, or for credit providers to disclose all available credit information to a credit reporting body.

Subclause (3) deals with the interaction of this provision with APP 10. This provision makes clear that APP 10 does not apply to the credit provider in relation to credit eligibility information. However, APP 10 will continue to apply to a credit provider that is an APP entity in relation to any other personal information the credit provider may hold.

Clause 20N sets out additional obligations imposed on credit reporting bodies to enter agreements with credit providers dealing with certain matters and requiring credit providers to take appropriate steps to maintain the quality of credit reporting information. The purpose of these specific obligations is to ensure that both credit reporting bodies and credit providers take proactive steps in establishing practices that maintain the quality of credit information. These provisions are not mirrored in clause 21Q. The obligations on credit providers will be set and enforced by the agreements and it is only necessary to impose legislative obligations on credit reporting bodies, as part of their obligations to take steps to maintain the quality of credit reporting information, to enter into these agreements.

Clause 21R False or misleading credit information or credit eligibility information

This provision deals with disclosing false or misleading credit information or using or disclosing false or misleading credit eligibility information. It provides both an offence provision and a civil penalty provision to deal with this conduct in relation to both types of information and is based on clause 20P, which imposes a similar offence and civil penalty on credit reporting bodies. While civil penalty provisions have generally been used throughout the Bill to deal with situations in which breach of a provision warrants the imposition of a penalty, some kinds of conduct require the imposition of criminal penalties. Providing for both a criminal offence and a civil penalty in this provision, as in clause 20P, gives the courts appropriate options to deal with the behaviour, depending on the circumstances of each case.

Subclauses (1) and (2) set out offences. Subclause (1) states that a credit provider commits an offence if the provider discloses credit information under clause 21D (which deals with disclosure of credit information to a credit reporting body) and the information is false or misleading in a material particular. Subclause (2) states that a credit provider commits an offence if the provider uses or discloses credit eligibility information under this Division and the information is false or misleading in a material particular. The penalty for both of these offences is 200 penalty units.

Subclauses (3) and (4) set out the matching civil penalties. Subclause (3) states that a credit provider must not disclose credit information under clause 21D if the information is false or misleading in a material particular. Subclause (4) states that a credit provider must not disclose credit eligibility information under this Division if the information is false or misleading in a material particular. The civil penalty for breach of these provisions is 2000 penalty units.

Clause 21S Security of credit eligibility information

This provision is based on the obligations set out in APP 11, modified to apply specifically to credit providers. This provision is similar to the obligations imposed upon credit reporting bodies by clause 20Q. However, clause 20Q contained additional obligations to enter agreements with credit providers dealing with certain matters to maintain the quality of credit information. In addition, credit reporting bodies have specific obligations in relation to the retention and destruction of credit reporting information. Credit providers do not have the same specific obligations and the retention and destruction of credit eligibility information is dealt with by a general rule, based on APP 11, contained in this provision and supported by a civil penalty offence.

Subclause (1) provides that a credit provider that holds credit eligibility information must take such steps as are reasonable in the circumstances to protect the information from misuse, interference and loss, and from unauthorised access, modification or disclosure. These are fundamental obligations and no exceptions are provided for these obligations.

Subclause (2) deals with the retention and destruction, or de-identification, of credit eligibility information. Subclause (2) applies where a credit provider holds credit eligibility information, the provider no longer needs the information for any purpose for which the information may be used or disclosed by the provider under this Division, and the provider is not required by or under an Australian law, or a court or tribunal order, to retain the information. Where these conditions are met, the provider must take such steps as are reasonable in the circumstances to destroy the credit eligibility information or to ensure that the information is de-identified. The civil penalty for breach of this provision is 1000 penalty units.

The rule on retention of credit eligibility information provides guidance on when the information should no longer be retained. Retention is tied to whether a credit provider is able to use or disclose that information under this Division. If the credit provider can no longer use or disclose the information, then there is no reason to retain the information. For example, if a person has closed their credit account and there are no outstanding liabilities there would be no further use or disclosure of any credit eligibility information and the information should no longer be retained (unless the provider is required to retain the information by or under an Australian law or a court or tribunal order).

Consistent with APP 11, a credit provider has the option of destroying or de-identifying credit eligibility information when the information is no longer needed. De-identifying the information should be done in a way that ensures the information is no longer 'personal information'. This will include ensuring that the information, when associated with other information, cannot be used to identify an individual. Unlike the situation with credit reporting bodies, there are no specific rules about the use of de-identified credit eligibility information by credit providers.

Subclause (3) deals with the interaction of this provision with APP 11. This provision makes clear that APP 11 does not apply to the credit provider in relation to credit eligibility information. However, APP 11 will continue to apply to a credit provider that is an APP entity in relation to any other personal information the credit provider may hold.

Subdivision F – Access to, and correction of, information

Clause 21T Access to credit eligibility information

This provision is based on the obligations set out in, and the structure of, APP 12, modified to apply specifically to credit providers. It is generally intended that access to credit eligibility information should occur on the same terms as access to personal information held by an APP entity. This provision is similar to the obligations imposed upon credit reporting bodies by clause 20R.

Subclause (1) states the general obligation that if a credit provider holds credit eligibility information about an individual, the provider must, on request by an access seeker, give the access seeker access to the information. 'Access seeker 'is defined in clause 6L. In this context an access seeker means the individual to whom the credit eligibility information relates, or a person who is assisting the individual deal with the credit provider, or an agent of the individual (that is, a person who is authorised in writing by the individual for the purpose of clause 21T – note that the National Relay Service is specifically exempted from this requirement by subclause 6L(3)). The term is subject to certain exceptions set out in the definition.

This provision permits the individual to obtain access to their credit eligibility information. This includes the CP derived information about the individual (for example, any credit scoring or analysis about the individual). While the individual can obtain access to the CP derived information about them, this does not provide them with a right to access the methodology, data analysis methods, computer programs, or other information that the credit provider may use to manage their credit eligibility information or to analyse the credit reporting information to produce the CP derived information.

Subclause (2) sets out exceptions to access. This list of exceptions has been deliberately modified and reduced from the list of exceptions set out in APP 12.3, on the basis that there is a significant public interest in ensuring individuals have access to their credit eligibility information. These are the only grounds on which access can be refused. This provision states that the credit reporting body is not required to give access to the credit reporting

information to the extent that: giving access would be unlawful (whether under the Privacy Act or another enactment); denying access is required or authorised by or under an Australian law or a court or tribunal order; or giving access would be likely to prejudice one or more 'enforcement related activities' (a defined term – see schedule 1) by, or on behalf of, an 'enforcement body' (defined in the Act).

Subclause (3) states that a credit reporting body must respond to the request for access within a reasonable period after the request is made. While credit reporting bodies have a 10 day limit for response under clause 20R, no such defined period is stated for credit providers. This is due to the greater variety in the types of entities that may be 'credit providers', and recognises that a reasonable time for some credit providers will be based on their circumstances and the nature of their business, as with any APP entity providing access under APP 12. However, while no period is defined, it is expected that most credit providers would, like credit reporting bodies, reasonably be able to provide access within a 10 day period.

Subclause (4) deals with the means of access. It states that, if a credit reporting body gives access, the access must be given in the manner set out in the registered CR code. It is expected that the registered CR code will deal with procedural matters around providing access, such as the means of access, where and how access may be provided, and other related matters.

Subclauses (5) and (6) deal with access charges. Unlike credit reporting bodies, there is no obligation to provide individuals with free access to their information once every 12 months, unless the credit provider is an agency. Subclause (5) states that if credit provider is an agency, the provider must not charge an access seeker for making a request or for giving access to the information. Subclause (6) provides that, if a credit provider is an organisation or small business operator, any charge by the provider for giving access must not be excessive and must not apply to the making of the request. This is the same test that applies under APP 12.8. Distinguishing between agencies and organisations or small business operators is consistent with the rules established in APP 12.7 (for agencies) and APP 12.8 (for organisations).

Subclause (7) sets out the process of providing notice to the access seeker where access is refused. It provides that, where access is refused because of subclause (2) (which sets out the only exceptions to access), the credit provider must give the access seeker a written notice that sets out the reasons for the refusal. The obligation to provide reasons is limited to the extent that it would be unreasonable to do so, having regard to the grounds for the refusal. For example, where access to some of an individual's credit eligibility information is refused because it may prejudice an enforcement related activity, it may be unreasonable to set out the details of the law enforcement activity or even that the law enforcement activity has provided the basis for restricting access to a part of the individual's credit eligibility information.

Subclause (7) goes on to provide that the written notice provided to the access seeker must inform the access seeker that, if they are not satisfied with the response to the request, they may access a recognised external dispute resolution scheme of which the body is a member (and provide contact details for that scheme) or make a complaint to the Commissioner under Part V of the Act.

Subclause (8) deals with the interaction of this provision with APP 12. This provision makes clear that APP 12 does not apply to the credit provider in relation to credit eligibility

information. However, APP 12 will continue to apply to a credit provider that is an APP entity in relation to any other personal information the credit provider may hold.

Clause 21U Correction of credit information or credit eligibility information

Clauses 21U, 21V and 21W are based on the obligations set out in APP 13, modified, and with additional provisions, to apply specifically to credit providers. Read together, these three provisions set out a correction process that provides individuals with specific rights and deal with matters that are particularly important in the context of credit reporting, such as providing evidence to substantiate disputed personal information in the credit reporting system. Importantly, individuals are able to request the correction of their personal information that may not be held by the credit provider, requiring the credit provider to consult with the appropriate credit reporting body or another credit provider. The credit provider to which the individual first makes a correction request must deal with that request. This imposes a specific obligation on providers to assist individuals to correct their personal information, no matter whom it is held by in the credit reporting system. The industry participants in the credit reporting system derive significant benefits from the availability of information about individuals in the system and it is considered appropriate that they take on obligations to assist individuals to correct their information. These provisions are mirrored by clauses 20S, 20T and 20U which impose similar obligations on credit reporting bodies. The only differences between the two sets of provisions is that the credit provider provisions also deal with the interaction of each provision with the APPs, and the provisions apply to credit information or credit eligibility information.

Clause 21U sets out the general obligations on credit providers to correct credit information as well as credit eligibility information. The correction obligation is expressly linked to the obligations on credit providers to ensure the quality of the credit eligibility information they maintain. Subclause (1) provides that a credit provider must take reasonable steps (if any) to correct credit eligibility information that is inaccurate, out-of-date, incomplete, irrelevant or misleading. Correction should take into account the purpose for which the information is held. The purpose of holding information will depend on the provisions of this Division and the definitions, and this will then inform decisions about whether information may be inaccurate, out-of-date, incomplete, irrelevant or misleading (note that if at least one of these descriptions can be applied to an individual's credit eligibility information it must be corrected). For example, credit information may include an individual's current address and up to two previous addresses in the previous five years, if any. Holding the previous addresses does not mean that the credit provider has out-of-date information. However, address information may become out-of-date if, for example, the individual moves from their current address and the credit provider is made aware of this change, as the provider will now be required to up-date the address information.

Credit providers have a dual role, providing credit information into the credit reporting system and using credit eligibility information coming out of the credit reporting system. The obligations set out in clause 21U apply to both credit information (covering the role of providers in disclosing this information to credit reporting bodies and hence into the credit reporting system) and credit eligibility information.

Subclause (2) states that a credit provider who has corrected credit information or credit eligibility information that has previously been disclosed under this Division (with the exception of disclosure to consult on a correction request under subclause 21V(4)) must, within a reasonable period, give each recipient of the information written notice of the correction. This obligation is to ensure that other recipients are aware of the correction and can take appropriate action to up-date their own records. As recipients of an individual's

credit information or credit eligibility information may be making credit related decisions of significance for the individual (or, in the case of credit reporting bodies, providing the information to other recipients who are making such decisions), it is important that any corrections are transmitted quickly and efficiently. It is expected that the registered CR code will deal with notification periods and procedures.

Subclause (3) provides that the obligation for written notice under subclause (2) does not apply if it is impracticable for the credit provider to give the notice or the credit provider is required by or under an Australian law, or a court or tribunal order, not to give the notice. It is expected that it would generally always be practicable for a credit provider to give the notice, as providers must make written notes of any disclosures. However, there may be circumstances where it is impracticable to provide the notice, for example where another credit provider has ceased trading.

Subclause (4) deals with the interaction of this provision with APP 13. This provision makes clear that APP 13 only applies to credit information or credit eligibility information that is identification information. In every other case, APP 13 does not apply to credit information or credit eligibility information. However, APP 13 will continue to apply to a credit provider that is an APP entity in relation to any other personal information the credit provider may hold. The reason for providing a special rule for identification information is that this information is also the kind of personal information that a provider may hold and be related to personal information outside the credit reporting system. Where that is the case, an individual may correct the information under APP 13. The credit provider should then be able to itself correct the identification information that is held as part of the credit information or credit eligibility information. As set out in the note, the effect of this rule is that identification information may be corrected under APP 13 or under this clause, as part of the individual's credit information or credit eligibility information. The rule does not say that APP 13 is the only way to correct identification information – instead, the rule provides that APP 13 may also apply to the correction of such information.

Clause 21V Individual may request the correction of credit information etc.

This provision sets out the process by which an individual may request the correction of certain personal information about them which is held in the credit reporting system. An individual is able to make a request for the correction of their information to a credit provider and the provider must, if it does not hold the information or cannot be satisfied that the information should be corrected, take steps to consult another credit provider or a credit reporting body to assist in resolving the individual's request.

Subclause (1) provides that an individual may request a credit provider to correct specified kinds of personal information in the credit reporting system if the provider holds at least one of the specified kinds of personal information about the individual. The personal information about the individual that may be subject to a correction request may be credit information, CRB derived information, or CP derived information. While a credit provider will not hold CRB derived information, the provision permits an individual to make a correction request about this kind of information to the provider.

Subclause (2) states the obligation to correct the personal information if the credit provider is satisfied that it is inaccurate, out-of-date, incomplete, irrelevant or misleading. The correction must be made within 30 days from the day the request is made, or such longer time as the individual agrees in writing. It is expected that the registered CR code will deal in greater detail with the process around which extensions of time to respond to correction requests are proposed to the individual. However, it is generally expected that most requests

for correction should be resolved within the 30 days specified in this provision. The period of 30 days has been specified to provide adequate time for consultation to occur under subclause (3), so the fact that consultation is required should not in itself be grounds for a provider to request that the individual agree to a longer period for consideration of the correction request. Where consultation is not required, it is expected that the correction request would ordinarily be considered and resolved well within the 30 days. The correction and complaint processes have been streamlined so that an individual can lodge a complaint with the Commissioner or a recognised external dispute resolution service immediately upon receiving notice of a refusal to make the requested correction under clause 20U. Accordingly, it is considered that a maximum period of 30 days in all but unusual cases should not present an unreasonable delay for the individual to have their correction request considered and resolved.

Where the personal information is corrected by the credit provider after consultation with another credit provider, then the notice obligations set out in clause 21W will operate. Any interested party consulted must be given notice of the correction. Those interested parties would be required to correct any personal information they hold or maintain to which the notice of correction relates by the operation of clause 20S (for a credit reporting body) or clause 21U (for a credit provider), which requires bodies or providers to ensure certain personal information they hold or maintain is not inaccurate, out-of-date, incomplete, irrelevant or misleading.

Subclause (3) deals with the process where the credit provider must consult so that it can be satisfied of the matter raised in the correction request. A credit provider may consult an interested party, which is either or both of another credit provider or a credit reporting body about the individual's request. However, the credit provider can only consult an interested party that has an Australian link, consistent with the limitation of the credit reporting system to Australia.

Subclause (4) authorises the use or disclosure of personal information about the individual for the purposes of consultation under subclause (3). As this information is being used or disclosed because it may not be correct, exceptions exist in other provisions in relation to quality obligations.

Subclause (5) states that the credit provider must not charge the individual for the making of the correction request or for correcting the information.

Subclause (6) deals with the interaction of this provision with APP 13. This provision makes clear that APP 13 only applies to personal information referred to in paragraph (1)(a) that is identification information. In every other case, APP 13 does not apply to personal information referred to in that paragraph. However, APP 13 will continue to apply to the credit provider in relation to any other personal information the credit provider may hold. This is the same rule as set out in clause 21U. As set out in the note, the effect of this rule is that identification information may be corrected under APP 13 or under this clause. The rule does not say that APP 13 is the only way to correct identification information – instead, the rule provides that APP 13 may also apply to the correction of identification information.

Clause 21W Notice of correction etc. must be given

This provision sets out the notice requirements that apply where the credit provider corrects, or does not correct, an individual's personal information.

Subclause (1) states that this provision applies if an individual requests a credit provider to correct personal information under subclause 21V(1).

Subclause (2) deals with notice requirements where a credit provider has corrected the individual's personal information. The credit provider must, within a reasonable time, give written notice of the correction to: the individual; to any interested party that the body consulted about the individual's correction request; and, where the information has been previously disclosed under this Division (except in relation to a correction request under subclause 20T(4) – in which case, anyone consulted must be given written notice)or the APPs (except in relation to APP 4.2, which deals with the collection of unsolicited information), to each recipient of the information. However, subclause (4) states that notice of all recipients is not necessary if it is impracticable for the credit reporting body to give the notice. It may be impracticable to give notice in situations where, for example, the recipient of the information has ceased trading. It is expected that it would generally always be practicable for a credit provider to give the notice, as providers must make written notes of any disclosures.

Subclause (3) deals with notice requirements where a credit provider does not correct the personal information as requested. The credit provider must, within a reasonable time, give the individual written notice: stating that the correction has not been made; setting out the provider's reasons for not correcting the information; and informing the individual that, if they are not satisfied with the provider's response to the request, the individual may access a recognised external dispute resolution scheme of which the provider is a member or make a complaint to the Commissioner under Part V of the Act. When the provider sets out its reasons for not correcting the information, the provider is required to include evidence substantiating the correctness of the information. This substantiation requirement means that the onus of proving the correctness of information that has been challenged by an individual rests with the provider (which, through the consultation requirements in clause 20T, can obtain substantiation evidence from another credit provider or credit reporting body). The evidence that should be provided to substantiate the correctness of the personal information will depend upon the circumstances. It is expected that this substantiation requirement will assist in resolving disputes quickly and efficiently. If evidence substantiating the information cannot be produced it is very unlikely that the provider would not be satisfied that the information should not be corrected as requested by the individual. In such circumstances the general obligations to maintain accurate, up-to-date and complete information will operate in support of the obligations to correct the information.

Subclause (5) sets a general exception to the notice obligations in subclauses (2) and (3) if the credit provider is required by or under an Australian law or a court or tribunal order not to give the notice.

Division 4 – Affected Information recipients

This Division deals with 'affected information recipients'. This term is used to refer collectively to various entities and persons to which credit reporting bodies or credit providers may disclose 'regulated information'. These entities and persons are:' mortgage insurers'; 'trade insurers'; a 'related body corporate' of a credit provider; a person who manages credit for a credit provider ('managing credit' is a defined term relevant to understanding the meaning of a person who is a credit manager); and an entity, legal adviser or financial adviser of a credit provider to whom information is disclosed in relation to the assignment of debts. The purpose of regulating these recipients is to ensure that they are subject to appropriate obligations in relation to their participation in the credit reporting system. In general, regulated information is disclosed to these recipients for specific and limited purposes and these provisions ensure the information is only used or disclosed for these purposes. These provisions also ensure that these recipients have appropriate privacy

policies in place in relation to this information and provide appropriate notice to individuals about certain matters in their privacy policies. These obligations are consistent with those imposed upon credit reporting bodies and credit providers.

'Regulated information' refers collectively to the kinds of information that may be disclosed to affected information recipients. Not every recipient can collect the same kind of information, so this term is necessary. Where it is necessary to refer to the particular kinds of information covered by this term, the following provisions do so. Every affected information recipient, except for trade insurers, may be the recipient of credit eligibility information from a credit provider. An affected information recipient that is a trade insurer may only be the recipient of credit reporting information from a credit reporting body. An affected information recipient that is a mortgage insurer may (in addition to receiving credit eligibility information from a credit provider) also be the recipient of credit reporting information from a credit reporting body.

Clause 22 Guide to this Division

This provision provides a guide to the Division.

Subdivision A – Consideration of information privacy

Clause 22A Open and transparent management of regulated information

Clause 22A is based on the obligations set out in APP 1, modified to apply specifically to affected information recipients and their handling and management of regulated information. The interaction of this provision with APP 1 is dealt with in subclause (7). This clause mirrors the obligations imposed on credit reporting bodies by clause 20B and credit providers by clause 21B.

Subclause (1) states the object of the provision.

Subclause (2) imposes a general requirement on affected information recipients to take reasonable steps to implement practices, procedures and systems in relation to their functions or activities as a recipient that will ensure compliance with: the requirements of the Division and the registered CR code (if it binds the recipient); and to enable them to deal with inquiries or complaints about their compliance. It is anticipated that affected information recipients will demonstrate their compliance with this obligation by, for example, developing and maintaining training programs, staff manuals, standard procedures and other relevant documents that demonstrate awareness of, and compliance with, their obligations under the Division and the registered CR code. In addition, affected information recipients should be able to demonstrate that their business systems, such as their data management systems, comply with the requirements of the Division or the registered CR code.

Subclause (3) requires affected information recipients to have a policy dealing with their management of regulated information. The policy must be clearly expressed and up-to-date.

Subclause (4) provides a list of matters on which the policy must contain information. The list is not exhaustive and the policy can, and should where necessary to satisfy the obligation set out in subclause (3), contain additional information. The purpose of the list is to provide guidance to affected information recipients on information that the policy must contain which is likely to be directly relevant to individuals and their concerns about the information handling practices of affected information recipients. It is not intended that the policy set out matters such as detailed operational or administrative procedures or the processes of internal data management systems, nor is it intended that the policy establish technical data handling standards.

Subclause (5) requires affected information recipients to take reasonable steps to make the policy publicly available. Affected information recipients must take reasonable steps to make the policy available free of charge, and must make the policy available in an appropriate form – for example, on their website.

Subclause (6) ensures that the policy is readily accessible to the public. While an affected information recipient may decide to make the policy available on their website, there may be circumstances where a person or body may wish to have the policy in a particular form – for example, in a different digital form that is more accessible for readers with a disability, or as a printed booklet. Following any such request, affected information recipients must take reasonable steps to provide the person or body with a copy of their policy in the requested form.

Subclause (7) deals with the interaction of this provision with the APPs. It makes clear that APPs 1.3 and 1.4 (which deal with privacy policies) do not apply to the affected information recipient in relation to regulated information. However, the APPs will continue to apply to an affected information recipient that is an APP entity in relation to any other personal information.

Subdivision B – Dealing with regulated information

Clause 22B Additional notification requirements for affected information recipients

Notification requirements apply to credit providers upon collection of personal information (see clause 21C). Notification requirements do not apply to credit reporting bodies as they do not collect personal information directly from individuals. Instead, clause 21C addresses this by requiring credit providers to notify individuals of certain matters in relation to the credit reporting bodies to which they disclose credit information. The intention of clause 22B is to ensure that affected information recipients that are APP entities that collect regulated information should also be subject to notification requirements. It is important that individuals know which entities have, or might have, their personal information and how they can access, correct or complain about that information in the hands of whichever entity holds the personal information. It is recognised that affected information recipient are in a similar position to credit reporting bodies, in that they do not collect regulated information, which is personal information, directly from the individual. However, APP 5 requires notice to be given at the time of collection, before the time of collection, or where either of these is not practicable, as soon as possible after the time of collection. The APP entity must take such steps as reasonable in the circumstances to provide the notification. It is expected that the most practical way for affected information recipients to comply with clause 22B will be to ensure that the required notice is provided to the individual before the affected information recipient collects the information from a credit reporting body or a credit provider. This could be done by, for example, the credit provider making the information available to the individual at the time of collection by the credit provider.

Clause 22B begins by establishing the notification obligations of affected information recipients that are APP entities. APP 5 imposes notification obligations upon APP entities upon collecting personal information. For the purposes of satisfying the notification requirements in APP 5.1 in relation to regulated information, the matters set out in paragraphs (a) to (c) must be notified to the individual and replace the matters set out in APP 5.2.

The affected information recipient must have a credit reporting privacy policy, as required by clause 22A. Individuals must be notified that the affected information recipient's policy contains information on how an individual may access, correct or make a complaint in

relation to regulated information about the individual, and how the affected information recipient will deal with such a complaint.

Clause 22C Use or disclosure of information by mortgage insurers or trade insurers

Disclosures of personal information may be made to mortgage insurers by credit reporting bodies (see clause 20F, which permits disclosure of credit reporting information, but it cannot include repayment history information – subclause 20E(4)) or credit providers (see clause 21L, which permits the disclosure of credit eligibility information, which can include repayment history information – paragraph 21G(5)(b)). Disclosures of personal information may be made to trade insurers by credit reporting bodies (see clause 20F, which permits disclosure of credit reporting information, but once again it cannot include repayment history information – subclause 20E(4)). Clause 22C sets out the rules for the use or disclosure of personal information held by mortgage insurers and trade insurers that has been disclosed to them under these provisions. Clause 22C is based on the obligations and structure of APP 6, but has been significantly modified.

Subclause (1) establishes a general prohibition on the use or disclosure of personal information about an individual by a mortgage insurer or trade insurer. The provision applies where the insurer currently holds personal information or previously held personal information about an individual. The personal information must have been disclosed to the insurer by a credit reporting body or a credit provider under Division 2 or 3. If these conditions are satisfied, the insurer must not use or disclose the information, or any personal information derived from the information. The inclusion of personal information that was previously held is necessary to ensure that any derived personal information that the insurer still holds, even though the insurer no longer holds the information from which it was derived, is also caught by the prohibition. Breach of this prohibition is subject to a civil penalty of 2,000 penalty units.

Subclauses (2) and (3) provide exceptions to the prohibition in subclause (1). Subclause (2) sets out the permitted uses. Paragraph (2)(a) provides that a mortgage insurer is permitted to use the information if the use is for a 'mortgage insurance purpose' of the insurer in relation to the individual. A mortgage insurer may also use the information for any purpose arising under a contract for mortgage insurance between the credit provider and the insurer. Paragraph (2)(b) provides that a trade insurer is permitted to use the information for a 'trade insurance purpose' in relation to the individual. These permitted uses mirror the purposes for which credit reporting bodies or credit providers may disclose personal information to mortgage insurers or trade insurers (see clauses 20F and 21L respectively). Paragraph (2)(c) provides a general exception to the prohibition where the use by the mortgage or trade insurer is required or authorised by or under an Australian law or a court or tribunal order.

Unlike APP 6, no secondary uses of the information by a credit provider are permitted. Only those uses expressly provided in subclause (2) are permitted.

No specific disclosures of the information by mortgage or trade insurers are permitted. Subclause (3) only permits a mortgage insurer or a trade insurer to disclose the information if the disclosure is required or authorised by or under an Australian law or a court or tribunal order.

Subclauses (4) and (5) deal with the interaction of this provision with the APPs where the insurer is an APP entity. Subclause (4) makes clear that APPs 6, 7 and 8 (which deal with use and disclosure, direct marketing and cross-border disclosures) do not apply to the mortgage insurer or trade insurer in relation to the information. Subclause (5) provides that,

if the information is a government related identifier of the individual (for example, a driver's licence number), APP 9.2 (which deals with the use or disclosure of such identifiers) does not apply to the mortgage insurer or trade insurer in relation to the information. However, these APPs will continue to apply to the mortgage insurer or trade insurer (if the insurer is an APP entity) in relation to any other personal information the insurer may hold.

Clause 22D Use or disclosure of information by a related body corporate

Clause 22D sets out the rules for the use or disclosure of credit eligibility information held by a related body corporate where the information has been disclosed to the body corporate by a credit provider. In this case, the body corporate is treated as being able to use or disclose the information as if it were the credit provider. Clause 22D is based on the obligations and structure of APP 6, but has been significantly modified.

Subclause (1) sets out the prohibition on use and disclosure. This provision states that, if a body corporate holds or held credit eligibility information about an individual and the information was disclosed to the body corporate by a credit provider under paragraph 21G(3)(b), the body must not use or disclose the information, or any personal information derived from that information. The inclusion of information that was previously held is necessary to ensure that any derived personal information that the body corporate still holds, even though the body corporate no longer holds the credit eligibility information from which it was derived, is also caught by the prohibition. Breach of this prohibition is subject to a civil penalty of 1,000 penalty units.

Subclauses (2) and (3) provide exceptions to the prohibition in subclause (1). Subclause (2) states that the prohibition in subclause (1) does not apply to a use or disclosure by the body corporate if the body would be permitted to use or disclose the information under clause 21G if the body were the credit provider. This provision puts the body corporate in the same position as the credit provider that disclosed the information to it. The reason for this is that the two entities are part of a related corporate structure. Subclause (3) provides further clarification by stating that, for the purposes of determining whether a body corporate would be permitted to use or disclose the information, it can be assumed the body is the credit provider that either provided the relevant credit, or collected the relevant application for credit from the individual, as the case may be. This provision recognises that there are different circumstances in which the information can be used or disclosed and the provision deems the body corporate to be in the same position as the credit provider for the purposes of whichever provision is relevant in clause 21G. The uses and disclosures under clause 21G include the permitted CP uses and the permitted CP disclosures set out in clauses 21H to 21P.

Subclauses (4) and (5) deal with the interaction of this provision with the APPs where the related body corporate is an APP entity. Subclause (4) makes clear that APPs 6, 7 and 8 (which deal with use and disclosure, direct marketing and cross-border disclosures) do not apply to the body corporate in relation to the credit eligibility information. Subclause (5) provides that, if the information is a government related identifier of the individual (for example, a driver's licence number), APP 9.2 (which deals with the use or disclosure of such identifiers) does not apply to the body corporate in relation to the information. However, these APPs will continue to apply to the body corporate (if the body corporate is an APP entity) in relation to any other personal information the body corporate may hold.

Clause 22E Use or disclosure of information by credit managers

Clause 22E sets out the rules for the use or disclosure of credit eligibility information held by credit managers that has been disclosed to them by a credit provider. Clause 22E is based on the obligations and structure of APP 6, but has been significantly modified.

Subclause (1) sets out the prohibition on use and disclosure. This provision states that, if a person holds or held credit eligibility information about an individual and the information was disclosed to the person by a credit provider under paragraph 21G(3)(c) for use in managing credit provided by the provider, the person must not use or disclose the information, or any personal information derived from that information. The inclusion of information that was previously held is necessary to ensure that any derived personal information that the person still holds, even though the person no longer holds the credit eligibility information from which it was derived, is also caught by the prohibition. Breach of this prohibition is subject to a civil penalty of 1,000 penalty units.

Subclauses (2) and (3) provide exceptions to the prohibition in subclause (1). Subclause (2) sets out the permitted uses. Paragraph (2)(a) provides that the person is permitted to use the information in managing credit provided by the credit provider. These permitted uses mirror the purposes for which credit providers may disclose information to a person who is a credit manager (see subclause 21G(3)). Paragraph (2)(b) provides a general exception to the prohibition where the use by the person is required or authorised by or under an Australian law or a court or tribunal order.

Unlike APP 6, no secondary uses of the information by a credit manager are permitted. Only those uses expressly provided in subclause (2) are permitted.

No specific disclosures of the information by credit managers are permitted. Subclause (3) only permits a credit manager to disclose the information if the disclosure is required or authorised by or under an Australian law or a court or tribunal order.

Subclauses (4) and (5) deal with the interaction of this provision with the APPs where the credit manager is an APP entity. Subclause (4) makes clear that APPs 6, 7 and 8 (which deal with use and disclosure, direct marketing and cross-border disclosures) do not apply to the credit manager in relation to the credit eligibility information. Subclause (5) provides that, if the information is a government related identifier of the individual (for example, a driver's licence number), APP 9.2 (which deals with the use or disclosure of such identifiers) does not apply to the credit manager in relation to the information. However, these APPs will continue to apply to the credit manager (if the credit manager is an APP entity) in relation to any other personal information the credit manager may hold.

Clause 22F Use or disclosure of information by advisers etc.

Clause 22F sets out the rules for the use or disclosure of credit eligibility information held by certain recipients that has been disclosed to the recipients by a credit provider. Clause 22F is based on the obligations and structure of APP 6, but has been significantly modified.

Subclause (1) sets out the prohibition on use and disclosure. This provision applies if a recipient holds or held credit eligibility information about an individual and the information was disclosed to the recipient by a credit provider under subclause 21N(2). A recipient is an entity, or a professional legal adviser of the entity, or a professional financial adviser of the entity. In these circumstances, the recipient must not use or disclose the information, or any personal information derived from that information. The inclusion of information that was previously held is necessary to ensure that any derived personal information that the person still holds, even though the person no longer holds the credit eligibility information from which it was derived, is also caught by the prohibition. Breach of this prohibition is subject to a civil penalty of 1,000 penalty units.

Subclauses (2) and (3) provide exceptions to the prohibition in subclause (1). Subclause (2) sets out the permitted uses. Paragraphs (2)(a) and (b) provide that the recipient is permitted

to use the information for the purposes set out in subclause 21N(3). If the recipient is a professional legal adviser of the entity or a professional financial adviser of the entity, the information must also be used in their capacity as an adviser to the entity and in connection with advising the entity about a matter referred to in subclause 21N(3). Paragraph (2)(c) provides a general exception to the prohibition on use or disclosure where the use by the recipient is required or authorised by or under an Australian law or a court or tribunal order.

Unlike APP 6, no secondary uses of the information by a recipient are permitted. Only those uses expressly provided in subclause (2) are permitted.

No specific disclosures of the information by recipients are permitted. Subclause (3) only permits a recipient to disclose the information if the disclosure is required or authorised by or under an Australian law or a court or tribunal order.

Subclauses (4) and (5) deal with the interaction of this provision with the APPs where the recipient is an APP entity. Subclause (4) makes clear that APPs 6, 7 and 8 (which deal with use and disclosure, direct marketing and cross-border disclosures) do not apply to the recipient in relation to the credit eligibility information. Subclause (5) provides that, if the information is a government related identifier of the individual (for example, a driver's licence number), APP 9.2 (which deals with the use or disclosure of such identifiers) does not apply to the recipient in relation to that information. However, these APPs will continue to apply to the recipient (if the recipient is an APP entity) in relation to any other personal information the recipient may hold.

Division 5 – Complaints

The procedures set out in this Division deal with complaints by individuals to credit reporting bodies and credit providers. However, this Division does not apply to complaints that follow a decision by a credit reporting body or a credit provider to refuse to provide access to, or correct, personal information as requested by the individual (or an access seeker authorised in writing by the individual). In these circumstances, an individual may complain directly to the Commissioner and the Commissioner must investigate the complaint (see subsection 40(1B), inserted by item 77 in Schedule 4 of the Bill).

Individuals may also choose to exercise their rights to complain to a 'recognised external dispute resolution scheme' of which a credit reporting body or credit provider is a member. An individual may then decide to lodge a complaint with the Commissioner under Part V of the Act. Subsection 40(1A) provides that the Commissioner must not investigate a complaint if it was not made to the respondent first, unless the Commissioner decides it was not appropriate to do so. In addition, paragraph 41(1)(dd) (inserted by item 85 in Schedule 4 of the Bill) permits the Commissioner to decide not to investigate a complaint because it would be more effectively or appropriately dealt with by a recognised external dispute resolution scheme. In most cases it is expected that the individual will complain to a credit reporting body or credit provider using the provisions in this Division, then complain to a recognised external dispute resolution scheme, then to the Commissioner.

An individual can complain to a credit reporting body or a credit provider about an act or practice of that credit reporting body or credit provider. This means, for example, that an individual is not able to complain to a credit provider about an act or practice of another credit provider. This is in distinction to the correction provisions, where an individual can make a correction request to any credit reporting body or credit provider and the recipient of the correction request must assist the individual to resolve the request, even if the recipient does not itself hold or maintain the personal information that is the subject of the request. When it comes to a complaint to a credit reporting body or credit provider, the complaint

must relate to the recipient credit reporting body or credit provider (noting that complaints about refusal of access or correction requests may be made directly to the Commissioner). Once an individual has made a complaint that relates to an act or practice of a credit reporting body or credit provider, that body or provider cannot refuse to accept the complaint and must, where it is necessary, consult one or more credit reporting bodies or credit providers, as appropriate, to reach a decision about the complaint. It is not possible for a credit reporting body or credit provider that has received a complaint to refer the complaint to another credit reporting body or credit provider for resolution.

The complaints process is subject to an important exception. This Division does not deal with complaints about a decision by a credit reporting body or a credit provider not to provide access to an individual or not to correct the individual's personal information following an access request or a correction request. In these circumstances the credit reporting body or credit provider has already made a decision about the request and provided the individual with reasons (unless an exemption applies) and, in the case of a correction request that has been refused, evidence substantiating the information. The individual is informed, as part of the notification provided to the individual about the refusal, of their right to complain directly to a recognised external dispute resolution service or the Commissioner, without the need for further complaint to the credit reporting body or credit provider about the refusal. However, if the individual considers that the credit reporting body or credit provider has not taken reasonable steps to ensure that the relevant personal information that the credit reporting body or credit provider collects, use or discloses is accurate, up to date, complete and (in the case of information the credit reporting body or credit provider uses or discloses) relevant, or has not taken reasonable steps to correct information the credit reporting body or credit provider holds and is inaccurate, out-of-date, incomplete, irrelevant or misleading, the individual may make a complaint to a body or provider about the act or practice using these provisions. It is expected that individuals would use the provisions that allow them to make a correction request in order to have their information corrected, rather than the complaints provisions, since the provisions in relation to correction requests have a number of advantages. These include that it is not necessary for the credit reporting body or credit provider to hold the particular personal information which the individual seeks to have corrected, and the credit reporting body or credit provider is required to give the individual evidence substantiating the correctness of the information.

It is expected that the registered CR code will provide additional obligations dealing with practical matters. These matters may include, for example: the steps credit reporting bodies and credit providers should take to establish appropriate public contact officers to deal with individuals about complaints; procedures to identify when a complaint has been made by an individual; standards and processes around how a respondent will deal with a complaint, including the investigation of complaints; and establishing robust procedures between credit reporting bodies and credit providers to ensure timely and effective consultation when it is required.

Clause 23 Guide to this Division

This provision provides a guide to the Division.

Clause 23A Individual may complain about a breach of a provision of this Part etc.

Clause 23A deals with complaints under Part IIIA and related matters.

Subclause (1) provides that an individual may complain to a credit reporting body about an act or practice engaged in by the body that may be a breach of Part IIIA or the registered CR code in relation to the individual. However, the individual cannot make a complaint about an

access refusal (clause 20R) or a refusal of a correction request (clause 20T), nor can the individual make a complaint about a breach of any provisions in the registered CR code that relates to these clauses. Complaints about an access refusal or a refusal of a correction request, or the breach of any registered CR code provision that relates to these matters, should instead be made to the Commissioner under Part V or to the relevant recognised external dispute resolution service.

Subclause (2) deals with complaints to credit providers in the same terms as subclause (1). It provides that an individual may complain to a credit provider about an act or practice engaged in by the provider that may be a breach of Part IIIA or the registered CR code in relation to the individual. However, the individual cannot make a complaint about an access refusal (which in the case of credit providers is dealt with in clause 21T) or a refusal of a correction request (clause 21V), nor can the individual make a complaint about a breach of any provisions in the registered CR code that relates to these clauses. Complaints about an access refusal or a refusal of a correction request, or the breach of any registered CR code provision that relates to these matters, should instead be made to the Commissioner under Part V or to the relevant recognised external dispute resolution service.

Subclause (3) provides that, if an individual makes a complaint, they must specify the nature of the complaint that they are making. The level of detail required will depend on the circumstances but the individual should specify the nature of the complaint in sufficient detail to allow the credit reporting body or credit provider to determine how to deal with the complaint. It is not necessary for the complaint to be made in writing.

Subclause (4) provides that the complaint may relate to personal information that has been destroyed or de-identified. There may be circumstances in which an individual considers that obligations around the destruction or de-identification of their personal information have been breached. An individual may also wish to complain about an act or practice that relates to the time before the personal information was destroyed or de-identified. In addition, credit reporting bodies have restrictions imposed on them by clause 20M in relation to the use and disclosure of de-identified personal information and there may be circumstances in which an individual considers that these obligations have been breached in relation to their personal information, including their personal information that has been de-identified.

Subclause (5) provides that a credit reporting body or a credit provider must not charge an individual for making a complaint or for dealing with the complaint.

Clause 23B Dealing with complaints

Once a credit reporting body or a credit provider receives a complaint they are the respondent to the complaint. This provision sets out the procedures and time frames that the respondent must comply with in dealing with a complaint.

Subclause (1) provides that once an individual has made a complaint, the respondent must give the individual a written notice that sets out certain matters. The respondent must provide the notice within 7 days after the complaint is made. This is a maximum time frame and it is expected that the notice could frequently be provided immediately upon receipt of the complaint – for example, where the complaint is made in person to the respondent, or where the complaint is made by a dedicated email or internet service. The written notice must acknowledge that the individual has made a complaint and set out how the respondent will deal with the complaint (including sufficient detail to inform the individual of the process that will be followed in dealing with the complaint). Subclause (1) concludes by imposing an obligation on the respondent to investigate the complaint.

Subclauses (2) and (3) provides that the respondent must undertake consultation about the complaint in certain circumstances. Subclause (2) provides that, if a respondent considers it necessary to consult a credit reporting body or credit provider about the complaint, the respondent must consult the body or provider. In relation to some complaints it may be necessary for the respondent to consult more than one credit reporting body or credit provider, and such consultation must occur. However, consultation is not required and should not be automatically undertaken without first considering the matter. It is a matter of judgement for the respondent to determine whether consultation is necessary as part of the respondent's investigation of the complaint. When making this judgement, the respondent should consider whether it has sufficient information to make a decision on the complaint. Once a decision has been made that consultation is necessary, the respondent must undertake that consultation.

Subclause (3) authorises the use or disclosure of personal information about the individual for the purposes of consultation under subclause (3). This provision ensures that personal information necessary for consultation on the complaint can be used or disclosed.

Subclauses (4) and (5) require the respondent to make a decision about the complaint within a specified time. Subclause (4) provides that the respondent must, after investigating the complaint, make a decision about the complaint and give the individual a written notice within the required time. The written notice must set out the decision and also inform the individual of their options if they are not satisfied with the decision. In this regard, if the respondent is a member of a recognised external dispute resolution scheme, the written notice must inform the individual that they may access the recognised external dispute resolution scheme, and that the individual may complain to the Commissioner under Part V of the Act.

Subclause (5) sets out the time frame for a decision under subclause (4). A decision must be made within 30 days, which starts from the day that the individual makes the complaint. However, if the individual has agreed to a longer period in writing, then the decision must be made within that longer period. It is expected that a decision would be made on most complaints within the 30 day period. The fact that a respondent decides consultation is required should not, of itself, be a reason for seeking the individual's agreement to a longer period in which to make the decision. It is expected that credit reporting bodies and credit providers will establish arrangements to quickly and efficiently consult and provide assistance in the investigation of an individual's complaint. It is expected that the registered CR code will contain further guidance on consultation procedures, as well as circumstances in which an individual would be asked to agree to a longer period and related matters.

Clause 23C Notification requirements relating to correction complaints

Clause 23C sets out certain notification requirements. The purpose of this provision is to ensure that other credit reporting bodies or credit providers know that a complaint has been received about certain personal information that they hold, to then inform them when the decision is made about the complaint, or to inform a body or provider that personal information which is disclosed to them is the subject of a complaint. The notification requirements are consistent with the obligations imposed upon credit reporting bodies and credit providers to ensure that personal information they collect, use or disclose is accurate, up-to-date, complete and (where the information is used or disclosed) relevant.

Subclause (1) states that this provision applies if an individual makes a complaint under clause 23A about an act or practice that may breach clause 20S (which sets out the correction obligations of credit reporting bodies) or 21U (which sets out the correction obligations of

credit providers). This means that these notification requirements apply where the complaint relates to the correction obligations of bodies or providers.

Subclauses (2) and (3) deal with notice requirements where a respondent has received a complaint about personal information that is held by a credit reporting body or credit provider. Subclause (2) applies to credit reporting bodies. If a body is the respondent to a complaint that relates to credit information or credit eligibility information that a credit provider holds, the body must notify the provider in writing of the making of the complaint as soon as practicable after it is made, and then notify the provider of the making of the decision about the complaint as soon as practicable after it is made. Where the decision results in changes to the personal information, the notice requirements in clause 20S require the body to inform every previous recipient of that personal information of the changes to the personal information. The credit reporting body will know which credit providers hold the changed personal information as the body is required to make written notes of all disclosures. While no specific time frame is provided, it is expected that as soon as practicable would generally mean as soon as the body was aware that a provider held the credit information or credit eligibility information that is the subject of the complaint.

Subclause (3) sets out requirements similar to subclause (2) for credit providers. Subclause (3) applies where a provider is the respondent to a complaint that relates to credit reporting information that a credit reporting body holds, or the complaint relates to credit information or credit eligibility information that another credit provider holds. In these circumstances, the provider must notify the body or the other provider in writing of the making of the complaint as soon as practicable after it is made, and then notify the body or the other provider of the making of the decision about the complaint as soon as practicable after it is made. Where the decision results in the changes to the personal information, the notice requirements in clause 21U require the provider would to inform the body or the other provider of any changes to the personal information. The credit reporting body will know which credit providers hold the changed personal information as the body is required to make written notes of all disclosures. While no specific time frame is provided, it is expected that as soon as practicable would generally mean as soon as the provider was aware that a body or other provider held the personal information that is the subject of the complaint.

Subclauses (4) and (5) deal with situations where personal information is disclosed that is the subject of a complaint that is unresolved. In these circumstances, the recipients of the personal information must be notified of the complaint. Subclause (4) applies to credit reporting bodies. Where a body discloses credit reporting information to which a complaint relates and a decision about the complaint has not been made, the body must notify the recipient of the information of the complaint. Subclause (5) applies to credit providers. The requirements apply where a provider discloses personal information which is disclosed either under Division 3 (which deals with credit providers) or under the APPs where the credit provider is also an APP entity. The reference to the APPs is necessary because some information, such as identification information, may be handled and maintained under either the credit reporting provisions or the APPs. If the provider discloses personal information to which a complaint relates and a decision about the complaint has not been made, the provider must notify the recipient of the information of the complaint.

Subclause (6) sets out two exceptions to the notice obligations in subclauses (2), (3), (4) and (5). The notice obligations do not apply if it is impracticable for the credit reporting body or the credit provider to give the notice. It may be impracticable to give notice in situations where, for example, the recipient of the information has ceased trading. In addition, the

notice obligations do not apply if a body or provider is required by or under an Australian law or a court or tribunal order not to give the notice.

Division 6 – Unauthorised obtaining of credit reporting information etc.

Clause 24 Obtaining credit reporting information from a credit reporting body

This provision prohibits entities from obtaining credit reporting information from a credit reporting body where the entity is not authorised to obtain the information or where the information is obtained by false pretences. It provides both an offence provision and a civil penalty provision to deal with this conduct. While civil penalty provisions have generally been used throughout the Bill to deal with situations in which breach of a provision warrants the imposition of a penalty, some kinds of conduct require the imposition of criminal penalties. Providing for both a criminal offence and a civil penalty in this provision gives the courts appropriate options to deal with the behaviour, depending on the circumstances of each case.

Subclauses (1) and (2) set out offences. Subclause (1) states that an entity commits an offence if the entity obtains credit reporting information from a credit reporting body and the entity is not an entity to which the body is permitted to disclose the information under Division 2, or an access seeker for the information. The penalty for this offence is 200 penalty units. An 'access seeker' is either an individual or someone who is assisting the individual to deal with a body and is authorised in writing by the individual, and is subject to certain limitations set out in the definition of the term. For example, in some circumstances an entity may be an access seeker on behalf of an individual and so may obtain credit reporting information in their capacity as access seeker that they would not otherwise have been entitled to receive under Division 2. In these circumstances, the entity has a legitimate reason for obtaining the information and should not be subject to an offence. Subclause (2) states that an entity commits an offence if the entity obtains credit reporting information from a credit reporting body and the information is obtained by false pretence. The penalty for this offence is 200 penalty units.

Subclauses (3) and (4) set out the matching civil penalties. Subclause (3) states that an entity must not obtain credit reporting information from a credit reporting body if the entity is not an entity to which the body is permitted to disclose the information under Division 2, or an access seeker for the information. The civil penalty for breach of this provision is 2000 penalty units. Subclause (4) states that an entity must not obtain, by false pretences, credit reporting information from a credit reporting body. The civil penalty for breach of this provision is 2000 penalty units.

Clause 24A Obtaining credit eligibility information from a credit provider

This provision mirrors clause 24 and prohibits entities from obtaining credit eligibility information from a credit provider where the entity is not authorised to obtain the information or where the information is obtained by false pretences. It provides both an offence provision and a civil penalty provision to deal with this conduct. While civil penalty provisions have generally been used throughout the Bill to deal with situations in which breach of a provision warrants the imposition of a penalty, some kinds of conduct require the imposition of criminal penalties. Providing for both a criminal offence and a civil penalty in this provision gives the courts appropriate options to deal with the behaviour, depending on the circumstances of each case.

Subclauses (1) and (2) set out offences. Subclause (1) states that an entity commits an offence if the entity obtains credit eligibility information from a credit provider and the entity is not an entity to which the provider is permitted to disclose the information under Division

3, or an access seeker for the information. The penalty for this offence is 200 penalty units. The reference to an 'access seeker' is included for the reasons set out in relation to clause 24. Subclause (2) states that an entity commits an offence if the entity obtains credit eligibility information from a credit provider and the information is obtained by false pretence. The penalty for this offence is 200 penalty units.

Subclauses (3) and (4) set out the matching civil penalties. Subclause (3) states that an entity must not obtain credit eligibility information from a credit provider if the entity is not an entity to which the provider is permitted to disclose the information under Division 3, or an access seeker for the information. The civil penalty for breach of this provision is 2000 penalty units. Subclause (4) states that an entity must not obtain, by false pretences, credit eligibility information from a credit provider. The civil penalty for breach of this provision is 2000 penalty units.

Division 7 – Court orders

This Division contains provisions that allow a court to make orders to compensate individuals in certain circumstances. The provisions are based on sections 178 and 179 of the National Consumer Credit Protection Act.

While it is the Commissioner that must apply to the court for a civil penalty order, the application for a compensation order must be made by the person claiming the compensation. In addition, the individual cannot apply to the court for a compensation order unless a civil penalty order has been made against the entity. This means that the individual's ability to apply for compensation is dependent on the Commissioner first applying for, and the court making, a civil penalty order. The provisions are structured in this way to ensure that an individual cannot use these provisions to force the Commissioner to bring a civil penalty order application in order to gain compensation. However, if the Commissioner brings an application for a civil penalty order relating to an act or practice of an entity, an individual is not prevented from making a complaint about the same act or practice and being afforded a remedy through conciliation or by a determination of the Commissioner.

Where a court finds that an entity has breached a civil penalty provision or an offence provision, the court may make an order of compensation to any person that has suffered any loss or damage as a result of that contravention. In addition to ordering monetary compensation, the court will also be able to make any other order that it considers appropriate to compensate the person or prevent or reduce the loss or damage suffered. These provisions provide the court with the option of considering compensation orders as part of the same court process for breach of the civil penalty or offence provision. This means that the court which has considered and made a decision about the breach may also choose to make compensation orders (where appropriate) at the same time. For example, this may be appropriate where an individual hasn't already received compensation following conciliation of a complaint relating to the same act or practice, or hasn't received compensation following a determination made by the Commissioner in relation to the same act or practice.

Clause 25 Compensation orders

Clause 25 provides for the making of compensation orders by the Federal Court or the Federal Magistrates Court.

Subclause (1) states that a court may order an entity to compensate a person for loss or damage suffered by the person, subject to the conditions set out in the provision. The loss or damage may include pecuniary loss or damage, but it is also clear that it may include non-pecuniary loss or damage, such as injury to the person's feelings or humiliation. An order may be made if a civil penalty order has been made against the entity for a contravention of a

civil penalty provision, or if the entity is found guilty of an offence against Part IIIA. In addition, loss or damage must have resulted from the contravention or commission of the offence. If, after satisfying these conditions, the court decides to order compensation, the order must specify the amount of compensation. An exception is provided for section 13G, which provides a civil penalty for serious and repeated breaches of privacy of one or more individuals, as a compensation order in these circumstances is not appropriate.

Subclause (2) provides that a court may only make a compensation order if the person applies for an order under this section and the application is made within 6 years of the day the cause of action that relates to the contravention or commission of the offence accrues.

Subclause (3) provides that, if the court makes the order, the amount of compensation specified in the order that is to be paid to the person may be recovered as a debt due to the person. This provision is intended to ensure that the person is subsequently able to take action, if necessary, to recover the amount of compensation from the entity.

Clause 25A Other orders to compensate loss or damage

Clause 25A provides for other orders that the Federal Court or the Federal Magistrates Court may make to compensate a person for loss or damage.

Subclause (1) sets out the circumstances in which the provision will operate. A civil penalty order must have been made against the entity for a contravention of a civil penalty provision, or the entity must have been found guilty of an offence against Part IIIA. An exception is provided for section 13G, which provides a civil penalty for serious and repeated breaches of privacy of one or more individuals, as a compensation order in these circumstances is not appropriate. The person must have suffered, or be likely to suffer, loss or damage, including injury to the person's feelings or humiliation, as a result of the contravention or commission of the offence. This provision provides the court with the option of making an order where the loss or damage is likely to occur, but hasn't yet been suffered.

Subclause (2) provides that the court may make such order as the court considers appropriate against the entity to compensate the person, whether in whole or in part, for the loss or damage, or to prevent or reduce the loss or damage suffered, or likely to be suffered, by the person.

Subclause (3) provides examples of orders that a court may make. The examples, which are based on some of the examples contained in section 179 of the National Consumer Credit Protection Act, are included to provide guidance to the court but are not intended to limit the court's power to make whatever order the court considers appropriate in the circumstances. The examples for consideration are an order directing the entity to: perform any reasonable act or course of conduct; pay reimbursement to the person; or pay the person the amount of loss or damage suffered.

Subclause (4) provides that the court may only make the order if the person applies for an order under this section and the application is made within 6 years of the day the cause of action that relates to the contravention or commission of the offence accrued.

Item 73 Subsections 30(3) and (4)

This item replaces references to 'credit reporting agency' in these subsections with 'credit reporting body'.

Item 74 Subsection 49(4) (paragraph (a) of the definition of *credit reporting offence*)

This item replaces cross-references in this subsection with the references to the new provisions in Part IIIA.

Item 75 Subsection 68(1)

This item replaces a reference to ‘credit reporting agency’ in this subsection with ‘credit reporting body’.

Schedule 3 – Privacy Codes

Notes on Clauses

Item 1 Subsection 6(1)

This provision inserts a cross-reference to the definition of 'APP code'.

Item 2 Subsection 6(1)

This provision inserts the definition of 'APP code developer'. The reference to APP entities means that both agencies and organisations can be an 'APP code developer'.

Item 3 Subsection 6(1) (definition of *approved privacy code*)

This provision repeals the definition as it has been replaced by the term 'APP code'.

Item 4 Subsection 6(1) (definition of *code complaint*)

This provision changes the references from approved privacy code to the new term, 'registered APP code'.

Item 5 Subsection 6(1) (definition of *Code of Conduct*)

This provision repeals the definition as it has been replaced by the 'CR code'.

Item 6 Subsection 6(1)

This provision inserts a cross-reference to the definition of 'Codes Register'.

Item 7 Subsection 6(1)

This provision inserts a cross-reference to the definition of 'CR code'.

Item 8 Subsection 6(1)

This provision inserts a definition of the term 'CR code developer'. This term is used to refer to the types of entity or entities that can be required to develop the CR Code by the Commissioner. A 'CR code developer' may be a single entity, a group of entities, or a body or association representing one or more entities. In every case, the proposed 'CR code developer' must be, or represent, an entity or entities that are subject to Part IIIA, which deals with credit reporting.

Item 9 Subsection 6(1) (definition of *credit provider*)

This provision inserts a reference to the new Part IIIB into the definition of 'credit provider'. This definition extends the meaning of 'credit provider' to include mortgage insurers and trade insurers, for specified purposes. Including the reference to Part IIIB means that mortgage and trade insurers will be included within the meaning of credit providers for the purposes of part IIIB, ensuring they can be bound by the CR Code, and must not breach that code.

Item 10 Subsection 6(1) (paragraph (a) of the definition of *credit reporting complaint*)

This provision changes the reference from Code of Conduct to the new 'registered CR code'.

Item 11 Subsection 6(1) (definition of *credit reporting infringement*)

This provision repeals the definition of credit reporting infringement as this term is no longer used. This term was previously used in paragraphs 13(1)(d) and 28A(1)(b). These provisions have been redrafted and expressed so that the content of the term 'credit reporting infringement' is used without the need to use the term itself.

Item 12 Subsection 6(1) (definition of *privacy code*)

This provision repeals the definition of privacy code, as this term is no longer used. It has been replaced by the term 'registered APP code'.

Item 13 Subsection 6(1)

This provision inserts a cross-reference to the definition of 'registered APP code'.

Item 14 Subsection 6(1)

This provision inserts a cross-reference to the definition of 'registered CR code'.

Item 15 Subsection 6(3A)

This provision repeals subsection 6(3A) because it is replaced by a new clause 6BA which achieves the same effect.

Item 16 At the end of subsection 6(7)

Subsection 6(7) recognises that in some circumstances a complaint may be relevant to more than one topic regulated by the Privacy Act. This provision inserts a new subsection to make clear that nothing prevents a complaint being both a complaint under the APPs and a 'code complaint'. The definition of 'code complaint' has been modified to refer to APP codes. It is a matter for the Commissioner to determine, under Part V of the Privacy Act, how to deal with a complaint that may be both an APP complaint and a code complaint.

Item 17 Section 6B (heading)

This provision changes the heading to refer to the new 'registered APP codes'.

Item 18 Subsections 6B(1), (2), (3) and (4)

This provision changes the references in these subsections from approved privacy codes to the new 'registered APP codes'.

Item 19 After section 6B

This provision inserts a new clause 6BA which replaces subsection 6(3A). It is located immediately after section 6B, which deals with breach of an APP code. Clause 6BA states that an act or practice will breach the registered CR Code if it is contrary to, or inconsistent with, the code. It is not necessary to insert the exemptions contained in subsections 6B(2) to (4) into this provision as the more specific nature of the credit reporting provisions and the CR Code means that there are not any circumstances in which those exemptions would operate.

Item 20 Subsection 7(2)

This provision changes the reference in the subsection from approved privacy codes to the new 'registered APP codes'. The policy intention of the provision is not changed.

Item 21 Subsection 7B(2) (note)

This provision changes the note to refer to the new registered APP codes.

Item 22 Subsection 13B(1) (note)

This provision changes the note to refer to the new registered APP codes.

Item 23 Subsection 13B(1) (paragraph (b) of the note)

This sentence in the note has been removed because, unlike privacy codes, the new APP codes cannot replace an APP so there cannot be a provision in a code that corresponds to (and replaces) an APP.

Item 24 Subsection 13B(1A) (note)

This provision changes the note to refer to the new registered APP codes.

Item 25 Subsection 13C(1) (note)

This provision changes the note to refer to the new registered APP codes.

Item 26 Subsection 13C(1) (note)

This sentence in the note has been removed because, unlike privacy codes, the new APP codes cannot replace an APP so there cannot be a provision in a code that corresponds to (and replaces) an APP.

Item 27 Division 5 of Part III

This provision repeals Division 5 of Part III. Division 5 deals with the CR Code of Conduct. This will be replaced with the new CR Code, provisions for which are contained in the new Part IIIB.

Item 28 Part IIIAA

This provision repeals part IIIAA, which deals with privacy codes. Privacy codes will be replaced with APP codes, provisions for which are contained in the new Part IIIB.

Item 29 Before Part IV

This provision inserts a new Part IIIB on Privacy codes. Part IIIB deals with APP codes and the CR Code.

Division 1 - Introduction

Clause 26 Guide to this Part

This provision is a guide to the Part.

Division 2 – Registered APP codes

Subdivision A – Compliance with registered APP codes etc.

Clause 26A APP entities to comply with binding registered APP codes

Once an APP entity is bound by a registered APP code, the APP entity must not do an act, or engage in a practice, that breaches that code. A breach of the registered APP code will be an interference with privacy by the entity under section 13 (inserted by schedule 4, item 6), about which a complaint can be made to the Commissioner under Part 5 of the Privacy Act.

Clause 26B What is a *registered APP code*

Subsection (1) has the effect that an APP code is only binding on an entity once it is registered on the Codes Register kept by the Commissioner. In addition, an APP code is only taken to be registered once it comes into force. An APP code must set out the period that it is in force as noted below.

To avoid any uncertainty, subsection (2) states that a registered APP code is a legislative instrument.

Subsection (3) provides that an APP code can take effect (come into force) before the date it is registered under the Legislative Instruments Act. However, an APP code cannot come into force before it is included on the Codes Register. This provision will provide certainty, for example, in circumstances where an APP code states that the period in which it is in force commences on the day it is included on the Codes Register, but there is a delay in registration under the Legislative Instruments Act. This means that there is a double registration process (on the Codes Register and then registration as a legislative instrument). Enabling an APP code to come into force upon registration by the Commissioner on a Codes Register maintained by the Commissioner ensures that the Commissioner retains control and responsibility for this important process.

Clause 26C What is an *APP code*

Subsection (1) makes clear that an 'APP code' must be in writing and must be about information privacy. It is not intended that an APP code would deal with matters unrelated to information privacy. However, it is also intended that the information privacy matters dealt with in the APP code are directly related to the APPs set out in the Privacy Act. There may be circumstances in which a code developer may wish to deal with other matters in a code, such as arrangements between APP entities that require consideration by another regulator, such as the Australian Securities and Investment Commission. To the extent that an APP code included matters that are not about information privacy, these matters would not form part of the APP code and would not be considered by the Commissioner. If a code developer wished to include other matters in an APP code it would be preferable to clearly identify the other matters and deal with them in a document separate to the APP code. That document would not form part of the APP code submitted to the Commissioner for approval and registration, nor would it form part of any registered APP code. Those matters would not be binding under the Privacy Act on entities bound by the APP code.

Subsection (2) states the matters that an APP code must deal with. These are the minimum requirements of every APP code. The first requirement is that an APP code must set out how one or more of the APPs are to be applied or complied with. This requirement addresses the fundamental purpose of APP codes, which is to provide detailed information on the application of, or compliance with, at least one APP. Depending on the circumstances, this may include setting out procedures that will be followed or even undertakings to comply with additional obligations that go beyond the requirements of an APP but which the entities subscribing to the APP code are willing to accept. This may be because, for example, the obligations represent a best practice commitment, or the obligations more accurately deal with particular circumstances in the industry, or the obligations address customer expectations in that industry. An APP code is not required to deal with all the APPs, although it may do so, but it must deal with at least one APP.

An APP code must also specify the APP entities that are to be bound by the code, or a way of identifying the entities bound by the code. Because an APP code is binding upon subscribers to the code it is essential that the code enables the subscribers to the code to be identified. This may be done, for example, by listing the subscribers to the code in the code document. However, there may be situations in which it is more effective for a code to describe a way in which entities that are bound by the code can be identified. For example, an industry association that develops a code for all members of that association may be able to describe all association members as being bound by the code. It will be a matter for the Commissioner to determine, when considering registration of the code, whether a way used to determine entities bound by the code is sufficiently clear and specific.

An APP code must set out the period during which the code is in force, and this period cannot start before the day on which the code is registered on the Codes Register. Clearly identifying the period which the code is in force is essential. It is not necessary for a code to commence operation on registration. For example, a code developer may wish to specify a specific commencement date for the code, or a specific time for commencement after registration of the code, to provide time for training of entities bound by the code, or for the development of materials or procedures under the code, or to provide time for additional entities to subscribe to the code. A code may be expressed to operate until a specified date or for a specified period, but it is expected that code developers will choose to state that the code continues in force until a specified event, such as the de-registration of the code.

Subsection (3) states the matters that an APP code may deal with. The purpose of this provision is to provide an indicative list of matters that may be included in a code, but a code is not required to include any of these matters. The list begins by stating that a code may impose additional requirements to those imposed by one or more of the APPs. This is intended to make clear that a code is not restricted to simply stating how an APP must be applied or complied with. However, if additional requirements that go beyond those contained in an APP are imposed, the additional requirements cannot be contrary to, or inconsistent with, any of the APPs. This is because an APP code cannot derogate from the obligations imposed by the APPs. Entities bound by a code must always comply with the APPs as well as the obligations imposed by the code to which they are bound.

A code can deal with exempt acts or practices of organisations that are exempt from the operation of the Privacy Act, as set out in sections 7B and 7C. In some circumstances an industry may choose to include obligations in an APP code that deal with acts or practices that would otherwise be exempt. For example, an industry may wish to include obligations in an APP code dealing with employee records, which are otherwise exempt from the Privacy Act under subsection 7B(3). However, only APP codes that are developed by an APP code developer can include provisions dealing with exempt acts and practices. The Commissioner is prevented from including exempt acts and practices in an APP Code that the Commissioner develops. In addition, the Commissioner cannot issue a request for code developers to include exempt acts or practices in a code, although if a code developer chooses to do so (in addition to dealing with the matters identified in the Commissioner's request) the Commissioner is able to consider and register a code containing provisions dealing with exempt acts and practices. Finally, the Commissioner cannot vary an APP code at his or her own initiative to insert provisions dealing with exempt acts or practices. However, the Commissioner may consider and approve an application for variation by an APP entity or entities bound by a code which deals with exempt acts or practices.

One important issue which APP code developers may wish to consider for inclusion in a code is the internal handling of complaints and reporting of complaints to the Commissioner. Code developers may wish to specify particular procedures or other matters that entities bound by the code will implement to ensure a consistent approach to the internal handling of complaints by all code subscribers. The internal handling of complaints refers to procedures, practices or processes that entities use to respond to complaints made to the entities. An APP code does not affect an individual's right to complain to the Commissioner or the process set out in the Privacy Act or used by the Commissioner to deal complaints. A code developer may wish to include provisions dealing with the reporting of complaints to the Commissioner, either as statistics, case notes, or in some other form. This may be done as a way of ensuring the Commissioner is aware of complaint numbers, issues and processes used by entities bound to a code containing such provisions.

An APP code may also deal with any other relevant matters. This makes clear that the list of matters does not limit the privacy issues that can be set out in an APP code. However, an APP code must deal with other relevant matters, and these other matters must be relevant to privacy in general and the APPs in particular. If a code developer decides to include matters that are not relevant to privacy or the APPs, such matters will not be considered as part of the APP code. It may be the case that code developers wish to deal with other matters of relevance to their industry or a type of technology. Such matters should be included in a separate document and will not be taken to be part of the APP code for approval by the Commissioner. In some circumstances these other matters may be issues for consideration by another regulator.

Subsection (4) states that an APP code may specify its application in various ways. An APP code is not required to deal specifically with any one or all of these matters. However, code developers may wish to consider these matters, and any other matters that could be specified to ensure that the intended objectives of the code can be clearly identified. Depending on the circumstances, it may be desirable for an APP code to specify the type of personal information to be covered by the code, whether any specified activities of an entity are subject to particular provisions of the code, whether the code will apply to a specified industry sector or profession, or a specified class of industry sectors or professions, or whether the code will apply to entities that use a specified type of technology. In relation to this last point, it is intended that an APP code can be specifically prepared to ensure entities use a specified technology in a way that applies, or complies with, their obligations under one or more of the APPs. For example, a code developer may wish to prepare a code that deals with one or more types of biometrics technologies which would be specified in the code.

Subsection (5) is declaratory and states that an APP code is not a legislative instrument. This is because an APP code is not enforceable until it is registered on the Codes Register. Once an APP code is registered on the Codes Register by the Commissioner and comes into force, it will at that point be a legislative instrument. It will therefore be required to be registered on the Federal Register of Legislative Instruments (FRLI).

Clause 26D Extension of Act to exempt acts or practices covered by registered APP codes

This provision only applies where a code covers exempt acts or practices and ensures certainty in relation to the application of the Privacy Act. The provision states that, if a registered APP code covers exempt acts or practices, the Privacy Act will apply to those acts or practices as if they were not exempt.

Subdivision B – Development and registration of APP codes

Clause 26E Development of APP codes by APP code developers

This provision sets out the process by which an APP code is developed by code developers. The specified circumstances in which an APP code can be developed by the Commissioner are set out in 18BE.

Subclause (1) states that an APP code developer may, at their own initiative, develop an APP code. The Commissioner may make guidelines relating to codes, set out in 18BJ, which may assist code developers in developing a code and provide guidance on the matters the Commissioner may have regard to in considering an application to register a code.

The remaining parts of this provision set out the rules under which the Commissioner may request a code developer to develop an APP code.

Subclause (2) states that the Commissioner may request an APP code developer to develop a code and apply for the code to be registered. In making such a request the Commissioner must be satisfied it is in the public interest for the code to be developed. It is a matter for the Commissioner to determine how to identify the appropriate code developer to which the request should be made. The term 'APP code developer' is defined to mean an APP entity, a group of APP entities, or an association or body representing one or more APP entities. Depending on the circumstances, the Commissioner may wish to target one APP entity as a code developer, or a group of entities, or a body or association. The Commissioner's request should be targeted in some way to a code developer, and should not take the form of a general public request for someone to develop an APP code.

Subclause (3) states that the Commissioner's request to develop an APP code must specify the period in which the code developer must comply with the request. The request cannot be open-ended. In addition, the request must set out the effect of section 18BA, which says that an APP entity must not do an act, or engage in a practice, that breaches a registered APP code that binds the entity. The purpose of including this reference is to ensure that the code developer is aware that an APP code is a binding instrument which contains enforceable obligations once registered.

Subclause (4) provides more detail on the period that must be specified for compliance with the request. The period must run for at least 120 days. This recognises that effective consultation with APP entities that are likely to be affected by the code, as well as other stakeholders, such as consumer representatives, is an important element in developing an effective code. Consultation will provide an opportunity to identify all relevant issues, options to address the issues, and likely effects on both APP entities that are bound by the code and others, such as consumers, who deal with these entities. This provision also provides the Commissioner with a general discretion to extend the period in which the request must be complied with. If necessary, the Commissioner could choose to extend the period one or more times, and for whatever period of time that the Commissioner considers appropriate in the circumstances.

Subclause (5) provides that the Commissioner may, in the request, specify one or more matters to that the code must deal with and the class of APP entities that should be bound by the code. Specifying such matters will provide guidance to the code developer on both the expected content of the code and who should be bound by the code, which may also assist the code developer in determining who should be consulted about the code in the development process. While it is not mandatory for the Commissioner to specify any such matters in the request, it is expected that in most cases the Commissioner would specify at least one matter the code must deal with. If the Commissioner chooses to specify such matters, it is a matter for the Commissioner to consider the amount of detail necessary to ensure that the request can be accurately and effectively addressed by the code developer.

Subclause (6) is consistent with the general policy that code developers can, at their own initiative, deal with exempt acts or practices, but cannot be directed to do so by the Commissioner. Where the Commissioner makes a request, the Commissioner cannot require the requested code to deal with exempt acts or practices. However, the code developer retains the discretion to include provisions dealing with exempt acts or practices if the code developer wishes to do so. If the code developer chooses to deal with exempt acts or practices, the Commissioner can consider those provisions along with the rest of the code provisions when the code developer applies for registration of the code.

Subclause (7) requires the Commissioner to make a copy of the request publicly available as soon as practicable after the request to the code developer is made. It is expected that

providing a copy of the request on a publicly available website, such as the website for the Office of the Australian Information Commissioner, would be sufficient to satisfy this requirement. Whether the Commissioner takes further steps to publicise the request – for example, by emailing contact lists to inform them of the request – is a matter for the Commissioner to determine in the circumstances.

Clause 26F Application for registration of APP codes

Subclause (1) permits an APP code developer to apply to the Commissioner for registration of the code. Registration of an APP code is at the discretion of the Commissioner, and the process by which the Commissioner determines whether to register an APP code is set out in section 18BF. It is also expected that the Commissioner will issue guidelines, as permitted by section 18BJ, to provide assistance to code developers in developing APP codes.

Subclause (2) sets out public consultation requirements that must be satisfied by the APP code developer before making an application to register the APP code. A draft of the APP code must be made publicly available, for example on a website of the code developer or some other relevant website. The code developer must invite the public to make submissions about the draft APP code and the period for submissions must run for at least 28 days to ensure that members of the public have sufficient time to consider the draft APP code. The 28 day consultation period is the minimum period that must be offered, but the code developer may consider a longer period, depending, for example, on the expected level of interest in the draft code, the number of expected stakeholders, the complexity of the code, or the expected impact of the provisions in the draft code on the practices or procedures of stakeholders. Although not specifically required, the code developer may also wish to bring the draft code to the attention of stakeholders, such as those entities that are expected to have an interest in participating in the draft code, as well as individuals, organisations or representative or advocacy associations (including consumer or privacy organisations that represent the interests of the community in relevant areas), amongst others, to ensure that they are aware of the public consultation period. The code developer must then consider any submissions which are made within the specified period. The code developer will need to be able to demonstrate compliance with these obligations when lodging an application for registration with the Commissioner.

Subclause (3) provides that an application for registration of an APP code must be made in the form and manner specified by the Commissioner and be accompanied by such information as is specified by the Commissioner. This provision allows the Commissioner to establish basic requirements for the way in which the draft code is provided and the form in which it is provided to the Commissioner. The Commissioner can also specify, for example, requirements that will assist the consideration of the application – such as the requirements for information that demonstrates the consultation requirements have been met by the Code developer.

Subclause (4) allows the code developer to vary the APP code at any time before the Commissioner registers the code with the Commissioner's consent. This provision is intended to allow the code developer to vary the draft code during the period in which the code is being considered by the Commissioner. This will allow the code developer to make variations that respond to concerns or comments made by the Commissioner. The variations must be agreed by the Commissioner. While the Commissioner cannot request that a code deal with exempt acts or practices, if a code developer decides to deal with exempt acts or practices in a code the Commissioner would be able to discuss and provide comments or views on the code developer's proposals in relation to exempt matters. If a code developer decides to vary provisions that deal with exempt matters, these variations can only be made

with the consent of the Commissioner. Even if variations are made to the code at the suggestion of, or in response to comments from, the Commissioner, this does not alter the Commissioner's discretion to register the draft code nor does it mean that the code developer is entitled to have the varied code registered.

Clause 26G Development of APP codes by the Commissioner

Subclause (1) sets out the circumstances in which the Commissioner can develop an APP code. The Commissioner can only develop an APP code in circumstances where a code developer has failed to comply with a request to develop a code, or where a code developer has produced a code as requested by the Commissioner, and the Commissioner has decided not to register the code. The Commissioner is not required to provide reasons for a decision not to register a code, but may choose to do so. There may be many circumstances where the Commissioner may decide not to register a code. This may be because the requested code does not deal adequately or effectively with the issues set out in the Commissioner's request or is defective in some other way. Alternatively, it may be because the consultation process was ineffective, the code developers failed to adequately consider public submissions received during the consultation period, or the code developers failed to comply with the requirements to provide the code in a form or manner, or accompanied by certain information, as requested by the Commissioner. It may also be the case that, on consideration of the code, the Commissioner does not consider that the provisions are effective when considered against the obligations set out in the APPs. In any event, having given the code developer the opportunity to develop an APP code, the Commissioner has the option of developing an APP code.

Subclause (2) sets out a public interest test. The Commissioner may develop an APP code if the Commissioner is satisfied it is in the public interest to do so. In considering the public interest, the Commissioner can consider the interests of stakeholders in an industry or activity, or the interests of certain segments of the public, as well as the public interest at large. The Commissioner must be satisfied that, overall, the public interest is served by development of the code. However, the Commissioner is prohibited from covering exempt acts or practices (as set out in sections 7B and 7C of the Privacy Act) if the Commissioner decides to develop an APP code. This is the case even if the Commissioner considers that it would be in the public interest to deal with exempt acts or practices in an APP code. It is not appropriate for the Commissioner to have the power to remove exemptions provided in the Privacy Act through the mechanism of an APP code that is imposed upon entities.

Subclause (3) sets out the consultation procedures the Commissioner must follow in the development of an APP code. A draft of the code must be made publicly available, for example on the Commissioner's website. The Commissioner must issue a public invitation to make submissions on the draft code within a specified period that must run for at least 28 days. The 28 day consultation period is the minimum period that must be offered, but the Commissioner may consider a longer period, depending, for example, on the expected level of interest in the draft code, the number of expected stakeholders, the complexity of the code, or the expected impact of the provisions in the draft code on the practices or procedures of stakeholders. Although not specifically required, the Commissioner may also wish to bring the draft code to the attention of stakeholders, such as those entities who are expected to be bound by the draft code, as well as individuals, organisations or representative or advocacy associations (including consumer or privacy organisations that represent the interests of the community in relevant areas), amongst others, to ensure that they are aware of the public consultation period. The Commissioner must then consider any submissions which are made within the specified period.

Clause 26H Commissioner may register APP codes

Subclause (1) states the Commissioner's discretion to register an APP code where the Commissioner has received an application for registration or where the Commissioner has developed an APP code. Registration occurs when the Commissioner registers the code by including it on the Codes Register, which the Commissioner is required to maintain by section 18BG.

Subclause (2) provides the Commissioner with the discretion to consult any person the Commissioner considers appropriate. The Commissioner may also consider any matters set out in any guidelines the Commissioner has issued under section 18BJ.

Subdivision C – Variation and removal of registered APP codes

Clause 26J Variation of registered APP codes

Subclause (1) provides the Commissioner with the power to approve, in writing, a variation of an APP code. A variation may be approved where the variation is prepared at the Commissioner's own initiative, or where an entity bound by the code applies for a variation, or where a body or association representing one or more entities bound by the code applies for a variation.

Subclause (2) states that, where the Commissioner decides to vary an APP code on the Commissioner's own initiative, the Commissioner is prohibited from including in that variation any provisions that deal with exempt acts or practices. However, where an application for a variation of an APP code is received from an entity, or a body or association representing one or more entities, bound by the code, the variation may deal with exempt acts or practices.

Subclause (3) sets out the consultation process the Commissioner must follow before deciding whether to approve a variation of an APP code. This is a simplified consultation process, recognising that the matter for consideration is a variation of an existing APP code. Unlike a consultation preceding the registration of a code, there is no statutory minimum consultation period. The variation must be made publicly available, for example on the Commissioner's website. The Commissioner must consult any person the Commissioner considers appropriate about the variation. For example, the Commissioner may decide to consult the entities bound by the APP code that will be affected by the variation. The Commissioner must also consider the extent to which members of the public have been given an opportunity to comment on the variation.

Subclause (4) sets out the procedure to be followed once a variation is approved by the Commissioner. The Commissioner must remove the original code from the Codes Register and register the APP code, as varied. This means that the variation itself is not registered. The whole APP code is replaced with a new version that incorporates the variation. This process is intended to ensure that there is no risk of confusion about the content of the registered APP code. The Codes Register will always contain the current version of an APP code.

Subclause (5) states that a variation comes into effect on the day specified in the approval. However, as registration is the act that ensures an APP code is enforceable, the variation cannot take effect before the whole APP code, as varied, is registered in the Codes Register.

Subclause (6) is declaratory and states that an approval of a variation of a registered APP code is not a legislative instrument. This is because the approval itself is not enforceable. Once the APP code, as varied, is registered on the Codes Register by the Commissioner the

varied APP code becomes enforceable. At that point it will be a legislative instrument, and will be required to be registered on the FRLI.

Clause 26K Removal of registered APP codes

Subclause (1) provides the Commissioner with the power to remove a registered APP code from the Codes Register. As with a variation, the Commissioner can remove a registered APP code at the Commissioner's own initiative, on the application of an entity bound by the code, or on the application of a body or association representing one or entities bound by the code. The Commissioner may choose to use the power to remove a registered APP code at his or her initiative where this is necessary, for example if the code no longer has any entities that subscribe to the code, or if the Commissioner considers the registered APP code is no longer effective.

Subclause (2) sets out consultation requirements the Commissioner must satisfy before removing a registered APP code from the Codes Register. The Commissioner must consult any person the Commissioner considers appropriate about the proposed removal. It is expected that this would include entities, if any, which continue to subscribe to the APP code. The Commissioner must also consider the extent to which the public has been given the opportunity to comment on the proposed removal. The provision does not require the publication of a notice about the proposed removal. The requirement to consult and consider the opportunity for the public to comment will allow the Commissioner to ensure that effective and appropriate public consultation has occurred.

Division 3 – Registered CR code

Subdivision A – Compliance with the registered CR code

Clause 26L Entities to comply with the registered CR code if bound by the code

This provision requires entities bound by the registered CR Code not to do an act, or engage in a practice, that breaches the code. This is similar to section 18BA, which deals with APP codes. A breach of the registered CR Code will be an interference with privacy by the entity under section 13 about which a complaint can be made to the Commissioner under Part 5 of the Privacy Act. The intention is that every entity which participates in the credit reporting system established by Part IIIA of the Act will be bound by the CR code as the code will deal with essential practical and operational matters for the operation of the credit reporting system.

Clause 26M What is the *registered CR code*

Subclause (1) has the effect that the registered CR code is the CR code that is included on the Codes Register kept by the Commissioner. It is not necessary to include a requirement that the CR code must set out the period that it is in force as the CR code is an essential component of the credit reporting system and it is expected that there will always be a CR code in force.

To avoid any uncertainty, subclause (2) declares that the registered CR code is a legislative instrument.

Subclause (3) provides that the CR code can take effect (come into force) before the date it is registered under the Legislative Instruments Act. However, the CR code cannot come into force before it is included on the Codes Register. This provision will provide certainty in circumstances where, for example, the CR code commences on the day it is included on the Codes Register, but there is a delay in registration under the Legislative Instruments Act.

Clause 26N What is a *CR code*

Subclause (1) makes clear that the CR code must be in writing and must be about credit reporting. It is not intended that the CR code would deal with matters unrelated to credit reporting. However, it is also intended that the credit reporting matters dealt with in the CR code are directly related to the credit reporting provisions set out in Part IIIA of the Privacy Act. There may be other matters which participants in the credit reporting system consider are also relevant to credit reporting and which the CR code developer may wish to deal with in the CR code. This might include agreements between entities that require consideration by another regulator, such as the Australian Securities and Investment Commission. To the extent that the CR code included such matters, these matters would not form part of the CR code and would not be considered by the Commissioner. If the code developer wished to include other matters in the CR code it would be preferable to clearly identify the other matters and place them in a document separate to the CR code. That document would not form part of the CR code submitted to the Commissioner for approval and registration, or any registered CR code. Those matters would not be binding under the Privacy Act on entities bound by the registered CR code.

Subclause (2) states the matters that the CR code must deal with. The first requirement is that the CR code must set out how one or more of the provisions of Part IIIA are to be applied or complied with. This requirement addresses the fundamental purpose of the CR code, which is to provide detailed information on the application of, or compliance with, the credit reporting provisions, including operational and practical matters.

The CR code is not required to deal with all the provisions of Part IIIA. However, there are provisions in Part IIIA which specify significant matters that must be contained in the CR code or matters which the CR code is permitted to address. It is expected that the CR Code would deal with all these matters.

The CR code must bind all credit reporting bodies. Credit reporting bodies are central to the operation of the credit reporting system and it is essential that they are bound by the CR code, which will set out in detail certain matters in relation to the application of, or compliance with, Part IIIA.

The CR code must also specify the credit providers, as well as any other entities subject to Part IIIA, that are to be bound by the CR code or a way of determining which credit providers or other entities are bound. Other entities that may be bound by the CR code include mortgage insurers and trade insurers. There may be situations in which it is more effective for the CR code to describe a way to determine which credit providers or other entities are bound, for example by identifying all members of an appropriate industry association. It will be a matter for the Commissioner to determine, when considering registration of the CR code, whether a way used to determine who is bound by the CR code is sufficiently clear and specific.

The intention is that every entity which participates in the credit reporting system established by Part IIIA of the Privacy Act will be bound by the CR codes. However, the different rules in the CR Code may apply in relation to only certain classes of entities subject to Part IIIA.

Subclause (3) states the matters that the CR code may deal with. The purpose of this provision is to provide an indicative list of matters that may be included in the CR code, but the CR code is not required to include any of these matters. The list begins by stating that the CR code may impose additional requirements to those imposed by Part IIIA. This is intended to make clear that the CR code is not restricted to simply stating how a requirement imposed by Part IIIA must be applied or complied with. However, if additional requirements that go

beyond those contained in Part IIIA are imposed, the additional requirements cannot be contrary to, or inconsistent with, Part IIIA. The CR code cannot derogate from the obligations imposed by Part IIIA. Entities bound by the CR code must always comply with Part IIIA as well as the obligations imposed by the CR code.

One important issue which the CR code developer may wish to consider for inclusion in the CR code is the internal handling of complaints and reporting of complaints to the Commissioner. Part IIIA contains specific obligations, rights and procedures in relation to certain credit reporting complaints. The code developer may wish to specify particular internal procedures or other internal complaint handling matters to ensure a consistent approach to credit reporting complaints by all entities bound by the CR code. Any complaint provisions in the CR code will not affect an individual's right to complain to the Commissioner or the process set out in the Privacy Act or used by the Commissioner to deal with complaints. The CR code developer may also wish to include provisions dealing with the reporting of credit reporting complaints to the Commissioner, either as statistics, case notes, or in some other form.

The CR code may also deal with any other relevant matters. However, the CR code must deal with matters that are relevant to credit reporting and, specifically, Part IIIA. If the CR code developer decides to include matters that are not relevant to credit reporting, such matters will not be considered as part of the CR code. The CR code developer may wish to deal with other matters of relevance to the credit reporting industry but not sufficiently related to the credit reporting provisions in Part IIIA. Such matters should be included in a separate document and will not be taken to be part of the CR code for approval by the Commissioner. If these other matters are issues for consideration by another regulator it is a matter for the CR code developer to seek approval from that other regulator for those matters.

Subclause (4) states that the CR code may be expressed to apply differently in relation to certain matters. Different rules may apply in relation to classes of entities subject to Part IIIA. This will allow, for example, specific rules to be provided in relation to certain types of credit providers, recognising their different interests in the credit reporting system. For example, specific rules may be provided for utilities or telecommunications service providers because of the different nature and circumstances of the credit they provide to their clients or because they may not have access to all categories of credit information (such as repayment history information because they are not licensees under the National Consumer Credit Protection Act). The CR code may apply differently in relation to specified classes of credit information, credit reporting information or credit eligibility information where there is a need for it to do so. The CR code may also apply differently in relation to specified classes of activities of entities subject to Part IIIA. The ability to develop different approaches in the CR code in these circumstances recognises that the CR code provisions that explain how the rules set out in Part IIIA may be applied or complied with may require specific guidance tailored to these matters. This provision provides the flexibility to deliver such detailed guidance.

Subclause (5) is declaratory and states that the CR code is not a legislative instrument. This is because the CR code is not enforceable until it is registered on the Codes Register. Once the CR code is registered on the Codes Register by the Commissioner and comes into force, it will at that point be a legislative instrument. It will therefore be required to be registered on the FRLI.

Subdivision B – Development and registration of CR code

Clause 26P Development of CR code by CR code developers

This provision sets out the process by which the CR code is developed by the CR code developer and is based on the process by which APP codes are developed as set out in section 18BC. The specified circumstances in which the CR code can be developed by the Commissioner are set out in 18ZC.

Subclause (1) states that the Commissioner may request a CR code developer to develop the CR code and apply for the code to be registered. The CR code is an essential part of the credit reporting regulatory scheme and it is anticipated that there will always be a CR code in place. However, as transitional provisions will deal with the development of the first CR code this provision provides a discretion rather than a mandatory requirement. The Commissioner may wish, at some point in the future to issue a request for a new CR code to be developed. It is a matter for the Commissioner to determine how to identify the appropriate code developer to which the request should be made. The term 'CR code developer' is defined in section 6 of the Privacy Act. The Commissioner's request should be targeted in some way to a CR code developer, and should not take the form of a general public request for someone to develop the CR code.

Subclause (2) states that the Commissioner's request must specify the period within which the CR code developer must comply with the request. The request cannot be open-ended. In addition, the request must set out the effect of section 18Z, which says that entities that are bound by the registered CR code must not do an act, or engage in a practice, that breaches the code that binds the entity. The purpose of including this reference is to ensure that the code developer is aware that the CR code is a binding instrument which contains enforceable obligations once registered.

Subclause (3)) provides more detail on the period that must be specified for compliance with the request. The period must run for at least 120 days. This recognises that effective consultation is an important element in developing the CR code and sufficient time must be provided to allow for the development of the CR code provisions and consultation to occur. The Commissioner also has a discretion to extend the period in which the request must be complied with. If necessary, the Commissioner could choose to extend the period one or more times, and for whatever period of time that the Commissioner considers appropriate in the circumstances.

Subclause (4) provides that the Commissioner may in the request specify one or more matters that the CR code must deal with and the class of credit providers or other entities subject to Part IIIA that should be bound by the code. Specifying such matters will provide guidance to the CR code developer on both the expected content of the CR code and who should be bound by the CR code, which may also assist the code developer in determining who should be consulted about the CR code in the development process. While it is not mandatory for the Commissioner to specify any such matters in the request, it is expected that the Commissioner would provide guidance on these matters. If the Commissioner chooses to specify such matters, it is a matter for the Commissioner to consider the amount of detail necessary to ensure that the request can be accurately and effectively addressed by the CR code developer.

Subclause (5) requires the Commissioner to make a copy of the request publicly available as soon as practicable after the request to the CR code developer is made. It is expected that providing a copy of the request on a publicly available website, such as the website for the Office of the Australian Information Commissioner, would be sufficient to satisfy this

requirement. Whether the Commissioner takes further steps to publicise the request – for example, by emailing contact lists to inform them of the request – is a matter for the Commissioner to determine in the circumstances.

Clause 26Q Application for registration of CR code

This provision is based on the process for application to register an APP code set out in section 18BD, as modified. Subclause (1) permits the CR code developer to apply to the Commissioner for registration of the code. Registration of the CR code is at the discretion of the Commissioner, and the process by which the Commissioner determines whether to register a CR code is set out in section 18ZD. It is also expected that the Commissioner will issue guidelines, as permitted by section 18BJ, to provide assistance to code developers in developing CR codes.

Subclause (2) sets out public consultation requirements that must be satisfied by the CR code developer before making an application to register the CR code. A draft of the CR code must be made publicly available, for example on a website of the CR code developer or some other relevant website. The CR code developer must invite the public to make submissions about the draft CR code and the period for submissions must run for at least 28 days to ensure that members of the public have sufficient time to consider the draft CR code. The 28 day consultation period is the minimum period that must be offered, but the CR code developer may consider a longer period. Although not specifically required, it may also be appropriate for a CR code developer to bring the draft CR code to the attention of stakeholders, as well as individuals, organisations or representative or advocacy associations (including consumer or privacy organisations that represent the interests of the community in relation to credit reporting), to ensure that they are aware of the public consultation period. The CR code developer must then consider any submissions which are made within the specified period. The CR code developer will need to be able to demonstrate compliance with these obligations when lodging an application for registration with the Commissioner.

Subclause (3) provides that an application for registration of the CR code must be made in the form and manner specified by the Commissioner and be accompanied by such information as is specified by the Commissioner. This provision allows the Commissioner to establish basic requirements for the way in which the CR code is provided and the form in which it is provided to the Commissioner. The Commissioner can also specify, for example, requirements that will assist the consideration of the application – such as the requirements for information that demonstrates the consultation requirements have been met by the CR code developer.

Subclause (4) allows the CR code developer to vary the CR code at any time before the Commissioner registers the CR code, but the variation must be done with the Commissioner's consent. This provision is intended to allow the CR code developer to vary the draft CR code during the period in which the CR code is being considered by the Commissioner. This will allow the CR code developer to make variations that respond to concerns or comments made by the Commissioner. The variations must be agreed by the Commissioner. Even if variations are made to the CR code at the suggestion of, or in response to comments from, the Commissioner, this does not alter the Commissioner's discretion to register the draft CR code nor does it mean that the CR code developer is entitled to have the varied CR code registered.

Clause 26R Development of CR code by the Commissioner

This provision is based on the process for the development of an APP code by the Commissioner set out in section 18BE, as modified. Subclause (1) sets out the circumstances in which the Commissioner can develop the CR code. The Commissioner can only develop

the CR code where a CR code developer has failed to comply with a request to develop the CR code, or where a CR code developer has produced a code as requested by the Commissioner, and the Commissioner has decided not to register the CR code. The Commissioner is not required to provide reasons for a decision not to register the CR code, but may choose to do so. There may be many circumstances where the Commissioner may decide not to register the CR code. This may be because the CR code does not deal adequately or effectively with the issues set out in the Commissioner's request or is defective in some other way. Alternatively, it may be because the consultation process was ineffective, the CR code developers failed to adequately consider public submissions received during the consultation period, or the CR code developers failed to comply with the requirements to provide the CR code in a form or manner, or accompanied by certain information, as requested by the Commissioner. It may also be the case that, on consideration of the CR code, the Commissioner does not consider that the provisions are effective when considered against the obligations set out in Part IIIA. In any event, having given the CR code developer the opportunity to develop the CR code, the Commissioner has the option of developing the CR code.

Unlike the development of an APP code by the Commissioner, a public interest test is not required. The CR code is a necessary part of the credit reporting regulatory scheme.

Subclause (2) sets out the consultation procedures the Commissioner must follow in the development of the CR code. A draft of the CR code must be made publicly available, for example on the Commissioner's website. The Commissioner must issue a public invitation to make submissions on the draft CR code within a specified period that must run for at least 28 days. The 28 day consultation period is the minimum period that must be offered, but the Commissioner may consider a longer period is appropriate. Although not specifically required, the Commissioner may also wish to bring the draft CR code to the attention of stakeholders as well as individuals, organisations or representative or advocacy associations (including consumer or privacy organisations that represent the interests of the community in relation to credit reporting), to ensure that they are aware of the public consultation period. The Commissioner must then consider any submissions which are made within the specified period.

Clause 26S Commissioner may register CR code

This provision is based on the procedures set out for the registration of APP codes in section 18BF, as modified. Subclause (1) states the Commissioner's discretion to register a CR code where the Commissioner has received an application for registration or where the Commissioner has developed a CR code. Registration occurs when the Commissioner registers the CR code by including it on the Codes Register, which the Commissioner is required to maintain by section 18BG.

Subclause (2) provides the Commissioner with the discretion to consult any person the Commissioner considers appropriate. The Commissioner may also consider any matters set out in any guidelines the Commissioner has issued under section 18BJ.

Subclause (3) requires the Commissioner to ensure that there is a registered CR code at all times after Part IIIA commences, and that there is only ever one CR code that is registered. The CR code is an essential component of the credit reporting regulatory scheme and this obligation ensures that the CR code must be in place at all times.

Subdivision C – Variation of the registered CR code

Clause 26T Variation of the registered CR code

This provision is based on section 18BH, as modified. Subclause (1) provides the Commissioner with the power to approve, in writing, a variation of the CR code. A variation may be approved where the variation is prepared at the Commissioner's own initiative, or where an entity bound by the CR code applies for a variation, or where a body or association representing one or more entities bound by the CR code applies for a variation.

Subclause (2) provides that an application under paragraphs (1)(b) or (c) for variation of an APP code must be made in the form and manner specified by the Commissioner and be accompanied by such information as is specified by the Commissioner. This provision allows the Commissioner to establish basic requirements for the way in which the draft code is provided and the form in which it is provided to the Commissioner. The Commissioner can also specify, for example, requirements that will assist the consideration of the application – such as the requirements for information that demonstrates the consultation requirements have been met by the Code developer.

Subclause (3) sets out the consultation process the Commissioner must follow before deciding whether to approve a variation of the CR code. The variation must be made publicly available, for example on the Commissioner's website. The Commissioner must consult any person the Commissioner considers appropriate about the variation. For example, the Commissioner may decide to consult the entities bound by the CR code that will be affected by the variation. The Commissioner must also consider the extent to which members of the public have been given an opportunity to comment on the variation. Unlike consultation preceding the registration of the CR code, there is no statutory minimum consultation period.

Subclause (5) sets out the procedure to be followed once a variation is approved by the Commissioner. The Commissioner must remove the original CR code from the Codes Register and register the new CR code, as varied. This means that the variation itself is not registered. The whole CR code is replaced with a new version that incorporates the variation. This process is intended to ensure that there is no risk of confusion about the content of the registered CR code. The Codes Register will always contain the current version of the CR code.

Subclause (6) states that a variation comes into effect on the day specified in the approval. However, as registration is the act that ensures the CR code is enforceable, the variation cannot take effect before the whole CR code, as varied, is registered in the Codes Register.

Subclause (7) is declaratory and states that an approval of a variation of the registered CR code is not a legislative instrument. This is because the approval itself is not enforceable. Once the CR code, as varied, is registered on the Codes Register by the Commissioner and comes into force, it will at that point be a legislative instrument. It will therefore be required to be registered on the FRLI.

Division 4 – General matters

Clause 26U Codes Register

APP codes, if any, and the CR code become effective on registration by the Commissioner in the Codes Register. The act of registration is essential for the codes to come into force and to be binding on the participants in the code. Subclause (1) requires to the Commissioner to keep the Codes Register. The Codes Register must include the APP codes and the CR code

the Commissioner has either decided to register or must register (depending on the relevant section in Part IIIB).

Subclause (2) deals with codes that have been removed pursuant to provisions in Part IIIB. The Commissioner is not required to include on the Codes Register an APP code or the CR code that has been removed from the Register.

Subclause (3) requires the Commissioner to make the Codes Register available on the Commissioner's website. This is to ensure that the Codes Register is freely and publicly available. It is also expected that the full content of any registered APP codes and the CR code would be available on the website and would be freely available to the public through the website.

Subclause (4) permits the Commissioner to charge fees for providing copies of, or extracts from, the Codes Register. It is expected that the Commissioner would charge reasonable fees, in keeping with the requirement to ensure information on the Codes Register is readily available to the public, and that fees would not be charged for public access to the Codes Register on the Commissioner's website.

Clause 26V Guidelines relating to codes

Subclause (1) provides the Commissioner with the power to make written guidelines relating to codes. The guidelines may provide assistance to APP or CR code developers on the development of the relevant codes. The guidelines may also provide assistance to relevant entities bound by an APP code or the CR code on how to apply or comply with the relevant code.

Subclause (2) provides the Commissioner with the power to make written guidelines about matters the Commissioner may consider in deciding whether to register or approve a variation of an APP code or the CR code, or to remove an APP code from the Codes Register.

Subclause (3) requires the Commissioner to publish any guidelines on the Commissioner's website to ensure the guidelines are publicly available.

Subclause (4) is declaratory and states that guidelines are not a legislative instrument. This is because the guidelines are not enforceable.

Clause 26W Review of operation of registered codes

Subclauses (1) and (2) provide that the Commissioner may review the operation of a 'registered APP code' or the 'registered CR code'. The note makes clear that any review which occurs may inform a decision by the Commissioner to approve a variation of a registered APP code or the CR code, or to remove a registered APP code from the Register. The review power is intended to ensure that the Commissioner can exercise an ongoing oversight role of the operation of registered APP codes and the CR code to ensure that the APP codes and the CR code continue to operate effectively and deal with relevant information privacy or credit reporting issues (as appropriate).

Item 30 Subsection 36(1)

This provision deletes the reference to subsection (1A) as it has been repealed.

Item 31 Subsections 36(1A), (1B) and (1C)

This provision repeals the subsections because they deal with privacy codes, which have been replaced by APP codes.

Item 32 Subsections 54(1A), 55A(7) and 55B(2)

This provision repeals the subsections because code adjudicators have been removed.

Item 33 Subsection 55B(3)

This provision removes the cross-reference to subsection (2), which has been repealed.

Item 34 Subsection 55B(3)

This provision removes the reference to adjudicator because code adjudicators have been removed.

Item 35 Subsection 55B(4)

This provision removes the cross-reference to subsection (2), which has been repealed.

Item 36 Subsection 64(1)

This provision renumbers the section.

Item 37 Subsection 64(2)

This provision repeals the subsection because code adjudicators have been removed.

Item 38 Section 95C

This provision changes the references from an ‘approved privacy code’ to a ‘registered APP code’, as APP codes have replaced privacy codes.

Schedule 4— Other amendments of the *Privacy Act 1988*

Introduction

The amendments in Schedule 4 will enhance the functions and powers of the Privacy Commissioner. The amendments will improve the Commissioner's ability to resolve complaints, recognise and encourage the use of external dispute resolution services, conduct investigations and promote compliance with privacy obligations.

The ALRC made a number of recommendations regarding reform of the functions and powers of the Privacy Commissioner. The ALRC adopted the notion of an outcomes-based or 'compliance-oriented' approach to regulation, in which all the factors of regulatory rule making, monitoring and enforcement are designed to elicit a particular regulatory objective. With its focus on achieving outcomes, the ALRC considered that compliance-oriented regulation provided a useful framework to administer a principles-based regime such as the Privacy Act.

The ALRC grouped the elements of compliance-oriented regulation under three concepts:

- securing or fostering voluntary compliance with the regulatory objectives
- undertaking informed monitoring for non-compliance, and
- engaging in enforcement actions where voluntary compliance fails.

In relation to the third element, the ALRC considered that in a compliance-oriented regulatory design, a regulator's response to non-compliance in a principles-based regime can be characterised as rehabilitative, rather than punitive. However, to be effective, attempts to nurture and restore compliance must operate in the presence of more punitive sanctions. The ALRC referred to this approach as an 'enforcement pyramid' approach, where a regulator can start with persuasive or restorative strategies and then move to more punitive strategies if voluntary compliance fails. Self-regulation and co-regulation also form part of the enforcement pyramid model.

The ALRC made a number of recommendations to strengthen the Privacy Commissioner's ability to foster and secure compliance in the first instance, monitor compliance as an ongoing concern, and enforce compliance where required. These were aimed at: providing for more efficient and effective enforcement of the Privacy Act; delivering efficient and effective complaint resolution; assisting the Commissioner to undertake proactive compliance actions; and enhancing the Commissioner's role in encouraging compliance outside of the Privacy Act's complaint-handling processes, including through privacy codes and audit powers. The Government accepted the majority of the ALRC's recommendations on the Commissioner's powers and functions.

The key objectives of the amendments in Schedule 4 are that:

- a compliance-oriented approach to the regulatory design of the provisions is taken which strengthens the Commissioner's ability to:
    - secure and foster voluntary compliance through both voluntary and mandatory mechanisms

- undertake monitoring for non-compliance, and
- engage in enforcement actions which are capable of escalation.

- the provisions take into account the Australian Information Commissioner Act and, where appropriate, provisions in the FOI Act are used as a model to draft comparable provisions in relation to specific reform proposals; and

- the provisions are consistent with the APPs and credit reporting provisions.

Item 1 After section 2

Item 1 will insert an objects clause into the Privacy Act as a new section 2A.

This amendment will implement ALRC Recommendation 5-4 with some modifications to the language and objects proposed by the ALRC. An objects clause will clearly outline the underlying purpose of the Act and provide assistance with interpretation.

The first two key objects are to promote the protection of privacy of individuals, while recognising that this protection should be balanced with the interests of entities in carrying out their legitimate functions or activities. The objects also include providing the basis for nationally consistent regulation of privacy and the handling of personal information, and the free flow of that information across national borders while respecting privacy. The objects are also to facilitate an efficient credit reporting system while respecting privacy, and promoting responsible and transparent handling of personal information. Finally, a key object of the Privacy Act is to implement Australia's international obligations in relation to privacy.

New section 29 (item 54 below) will require the Commissioner to have due regard to the objects of the Privacy Act in performing functions and exercising powers conferred by the Privacy Act.

Item 2 Subsections 5B(1) and (1A)

Item 2 will repeal and replace subsections 5B(1) and (1A).

The new subsection 5B(1) will extend the extra-territorial operation of the Privacy Act and registered APP and CR codes to agencies. Currently, section 5B does not deal with agencies. Extending the extra-territorial operation of the Privacy Act to agencies implements the Government's response to ALRC Recommendation 31-1.

The new subsection 5B(1A) is based on the old subsection 5B(1). It will provide that the Privacy Act operates extra-territorially in relation to organisations and small businesses that have an 'Australian link'.

The notes to new subsections 5B(1) and (1A) state that an act or practice overseas is not an interference with privacy if it is required by an applicable law of a foreign country.

Item 3 Subsection 5B(2) (heading)

Item 3 will repeal the heading 'Organisational link with Australia' to subsection 5B(2) and replace it with the heading 'Australian link'. The 'Australian link' expression is used to

define the entities that are subject to the operation of the Privacy Act. The expression is also used in a number of credit reporting provisions.

Item 4 Subsection 5B(2)

Item 4 will amend subsection 5B(2) by rephrasing the opening of the subsection and inserting a reference to the new term 'Australian link'. The list of entities in subsection 5B(2) has not been changed. The protection of the Privacy Act will extend to every person, not just Australian citizens or permanent residents, so long as the entity that is dealing with his or her personal information is an agency or an organisation with an Australian link.

Item 5 Subsection 5B(3) (heading)

Item 5 will repeal the heading to subsection 5B(3). The heading will no longer be necessary, given that both subsections 5B(2) and 5B(3) will define 'Australian link'.

Item 6 Subsection 5B(3)

Item 6 will amend subsection 5B(3) by rephrasing the opening of the subsection and inserting a reference to the new term 'Australian link'. This will clarify that the subsection lists additional connections with Australia which would be a sufficient link for the Privacy Act to operate extra-territorially in relation to organisations and small business operators under subsection 5B(1A).

The collection of personal information 'in Australia' under paragraph 5B(3)(c) includes the collection of personal information from an individual who is physically within the borders of Australia or an external territory, by an overseas entity.

For example, a collection is taken to have occurred 'in Australia' where an individual is physically located in Australia or an external Territory, and information is collected from that individual via a website, and the website is hosted outside of Australia, and owned by a foreign company that is based outside of Australia and that is not incorporated in Australia. It is intended that, for the operation of paragraphs 5B(3)(b) and (c) of the Privacy Act, entities such as those described above who have an online presence (but no physical presence in Australia), and collect personal information from people who are physically in Australia, carry on a 'business in Australia or an external Territory'.

Item 7 Paragraphs 5B(3)(a), (b) and (c)

Item 7 will amend paragraphs 5B(3)(a), (b) and (c) by including references to 'operators' as well as 'organisations'.

This will create consistency with an earlier amendment, which will provide that subsection 5B(3) applies to small business operators as well as organisations (item 6 above).

Item 8 Subsection 5B(4)

Item 8 will amend subsection 5B(4) by including a reference to subsection 5B(1A) alongside the reference to subsection 5B(1).

This will reflect an earlier amendment which provides that both subsections will have the effect of extending the Privacy Act's operation extra-territorially (item 2 above).

Item 9 Subsection 6(1)

Item 9 will insert a definition of 'advice related functions' into subsection 6(1).

The definition will refer to subsection 28B(1), which, as amended, will list the advice-related functions of the Commissioner.

Item 10 Subsection 6(1)

Item 10 will insert a definition of 'Australian link' into subsection 6(1).

The definition will refer to subsections 5B(2) and (3), which, as amended, will contain lists of connections with Australia sufficient to constitute an 'Australian link'.

Item 11 Subsection 6(1) (all the definitions of *breach*)

Item 11 will repeal and replace the definitions of 'breach' in subsection 6(1).

The new definition will refer to breach of an APP, replacing the two separate definitions in the current Privacy Act which refer to breach of an IPP and of an NPP. The definition will also refer to breaches of registered APP and CR codes under sections 6B and 6BA.

Item 12 Subsection 6(1)

Item 12 will insert a definition of 'civil penalty order' into subsection 6(1).

The definition will refer to new subsection 80W(4), which will provide that an order made under subsection 80W(3) is a civil penalty order (item 189 below).

Item 13 Subsection 6(1)

Item 13 will insert a definition of 'civil penalty provision' into subsection 6(1).

The definition will refer to section 80U, which will define civil penalty provisions as those sections or subsections with the words 'civil penalty' and one or more penalty unit amounts set out at their foot (item 189 below).

Item 14 Subsection 6(1) (definition of *code complaint*)

Item 14 will amend the definition of 'code complaint' in subsection 6(1) by removing the reference to a complainant and replacing it with a reference to an individual. This change is being made to include consistent and accurate terminology in the Privacy Act relating to complaints.

Item 15 Subsection 6(1)

Item 15 will insert a definition of 'committee of management' into subsection 6(1). This is a standard definition used in the case of unincorporated associations. New section 98B contains provisions outlining the treatment of unincorporated associations.

Item 16 Subsection 6(1) (definition of *credit reporting complaint*)

Item 16 will amend the definition of 'credit reporting complaint' in subsection 6(1) by removing the reference to a complainant and replacing it with a reference to an individual. This change is being made to include consistent and accurate terminology in the Privacy Act relating to complaints.

Item 17 Subsection 6(1)

Item 17 will insert a definition of 'Defence Department' into subsection 6(1). This is a more up-to-date drafting approach taken when referring to departments and agencies in legislation.

Item 18 Subsection 6(1) (definition of *file number complaint*)

Item 18 will amend the definition of 'file number complaint' in subsection 6(1) by removing the reference to a complainant and replacing it with a reference to an individual. This change is being made to include consistent and accurate terminology in the Privacy Act relating to complaints.

Item 19 Subsection 6(1) (paragraph (a) of the definition of *file number complaint*)

Item 19 will amend paragraph (a) of the definition of 'file number complaint' by removing the word 'guideline' and replacing it with the word 'rule'.

This change in terminology will implement the Government's acceptance of ALRC Recommendation 47-2. The word 'rule' will be used where appropriate throughout the Privacy Act to more accurately reflect the binding nature of certain guidelines and to distinguish binding instruments issued or approved by the Privacy Commissioner from voluntary guidance. This will also be reflected in an amendment to section 17 (item 51 below).

Item 20 Subsection 6(1)

Item 20 will insert a definition of 'guidance related functions' into subsection 6(1). The definition will refer to new subsection 28(1), which will list the guidance related functions of the Commissioner.

Item 21 Subsection 6(1) (definition of *individual concerned*)

Item 21 will repeal the definition of 'individual concerned' from subsection 6(1). That definition appeared in the former credit reporting provisions but has not been included in the new Part IIIA. It is therefore unnecessary to retain it.

Item 22 Subsection 6(1)

Item 22 will insert a definition of 'interference with the privacy of an individual' into subsection 6(1).

This definition will refer to new sections 13 to 13F, which will set out the circumstances in which an act or practice of various bodies will constitute an interference with the privacy of an individual.

Item 23 Subsection 6(1)

Item 23 will insert a definition of 'monitoring related functions' into subsection 6(1).

The definition will refer to subsections 28A(1) and (2) will list the monitoring related functions of the Commissioner.

Item 24 Subsection 6(1)

Item 24 will insert a definition of 'offence against this Act' into subsection 6(1). This is a standard criminal law provision that makes it clear that ancillary offences are included in offences against the Privacy Act.

Item 25 Subsection 6(1)

Item 25 will insert a definition of 'recognised external dispute resolution scheme' into subsection 6(1).

This definition will refer to new section 35A, which will provide that the Commissioner may recognise external dispute resolution schemes.

Item 26 Subsection 6(1) (definition of *tax file number information*)

Item 26 will amend the definition of 'tax file number information' in subsection 6(1) by removing the phrase '(including information forming part of a database)'. The reference to databases, which may have provided clarification in 1988 when the Privacy Act was passed, is no longer necessary and will not appear in the new definition.

Item 27 Subsection 6(3)

Item 27 will amend subsection 6(3) by removing the word 'guideline' and replacing it with the word 'rule'.

This change in terminology will implement the Government's response to ALRC Recommendation 47-2. The word 'rule' will be used where appropriate throughout the Privacy Act to more accurately reflect the binding nature of certain guidelines and to distinguish binding instruments issued or approved by the Commissioner from voluntary guidance. This will also be reflected in an amendment to section 17.

Item 28 Subsection 6(6)

Item 28 will amend subsection 6(6) by removing the reference to the Department of Defence and replacing it with the term 'Defence Department'.

This change in terminology reflects the new definition of 'Defence Department' which will be inserted into the Privacy Act (item 17 above).

Item 29 Paragraphs 7(1)(ca) and (g) and (1A)(c)

Item 29 will amend paragraphs 7(1)(ca) and (g) and (1A)(c) by removing the references to the Department of Defence and replacing them with the term 'Defence Department'.

This change in terminology reflects the new definition of 'Defence Department' which will be inserted into the Privacy Act (item 17 above).

Item 30 Subsection 7(2)

Item 30 will amend subsection 7(2) by removing the words 'under section 27' and replacing them with the phrase 'in relation to the principles and such a code'.

Removing the reference to section 27 will reflect a later amendment, which will repeal and replace section 27, and restructure the provisions dealing with the Commissioner's functions.

Item 31 Paragraph 7(2)(b)

Item 31 will amend paragraph 7(2)(b) by removing the reference to the Department of Defence and replacing it with the term 'Defence Department'.

This change in terminology reflects the new definition of 'Defence Department' which will be inserted into the Privacy Act (item 17 above).

Item 32 Subsection 7(3A)

Item 32 will repeal subsection 7(3A). This is essentially being reproduced in new subsection 12B(5).

Item 33 Subsection 7(4)

Item 33 will amend subsection 7(4) by removing a reference to certain paragraphs of section 27 and replacing it with a reference to section 28 and certain paragraphs of subsection 28A(2).

This will reflect a later amendment which will repeal and replace section 27 and restructure the provisions relating to the Commissioner's functions. The existing contents of the listed paragraphs of section 27, apart from paragraph 27(1)(g) which refers to the Personal Information Digest and is no longer applicable, are largely replicated in the new section 28 and the listed paragraphs of subsection 28A(2).

Item 34 Section 12B (heading)

Item 34 will repeal the heading to section 12B and replace it with a new heading: 'Severability – additional effect of Act'. This will remove the limiter 'in relation to organisations' from the section's heading. This is necessary because the provision is being extended to other entities.

Item 35 Subsections 12B(1) and (2)

Item 35 will repeal and replace subsections 12B(1) and (2). This is a severability provision which provides that the Privacy Act has effect in relation to certain regulated entities as provided for in subsections (2), (3), (4), (5), (5A), (6), (7) and (8). It is intended to ensure that the Privacy Act is given the widest possible operation consistent with Commonwealth constitutional legislative power. The Privacy Act has the effect it would have if its operation in relation to the entities mentioned in subsection (1) were expressly confined to:

- giving effect to the International Covenant on Civil and Political Rights, and in particular, Articles 17 and 24(1) of the Covenant
- giving effect to Article 16 of the Convention of the Rights of the Child
- acts or practices of regulated entities covered by sub-clause 5B(1) which occur outside Australia and the external Territories
- regulated entities which are corporations
- acts or practices of regulated entities taking place in the course of, or in relation to, trade or commerce between Australia and places outside Australia, among the States or within a Territory, between a State and a Territory or between two Territories
- acts or practices engaged in by regulated entities in the course of banking (other than State banking not extending beyond the limits of the State concerned), or insurance (other than State insurance not extending beyond the limits of the State concerned)
- acts or practices of regulated entities taking place using a postal, telegraphic, telephonic or other like service within the meaning of paragraph 51(v) of the Constitution
- acts or practices of regulated entities taking place in a Territory, and
- acts and practices of regulated entities taking place in a place acquired by the Commonwealth for public purposes.

Item 36 Subsection 12B(3)

Item 36 will amend subsection 12B(3) by replacing the word 'organisations' with the term 'regulated entities' to reflect the changes in terminology made as a consequence of extending the application of section 5B (extraterritorial effect).

Item 37 Subsection 12B(3)

Item 37 will amend subsection 12B(3) by removing the reference to subsection 5B(1) and replacing it with a reference to section 5B. This will reflect earlier amendments which mean that all of section 5B will deal with acts and practices outside Australia and the external Territories, rather than simply subsection 5B(1).

Item 38 Subsection 12B(3)

Item 38 will amend subsection 12B(3) by removing the limiting term 'by organisations'. This will reflect the fact that section 5B, as amended, will deal with agencies, organisations and small business operators, rather than just organisations.

Item 39 Subsection 12B(4) and (5)

Item 39 will amend subsections 12B(4) and (5) by replacing the word 'organisations' with the term 'regulated entities'. This is required because of the broader range of entities that are being regulated under the Privacy Act, particularly under the new credit reporting provisions.

Item 40 After subsection 12B(5)

Item 40 will insert a new subsection 12B(5A) after subsection 12B(5). This provision is intended to ensure that the Privacy Act is given the widest possible operation consistent with Commonwealth constitutional legislative power. This subsection makes it clear that the severability provision also relies on the banking and insurance powers in the Constitution.

This amendment provides that the Privacy Act has the effect it would have if its operation in relation to the entities mention in subsection (1) were expressly confined to acts or practices engaged in by regulated entities in the course of banking (other than State banking not extending beyond the limits of the State concerned), or insurance (other than State insurance not extending beyond the limits of the State concerned)

Item 41 Subsections 12B(6) to (8)

Item 41 will amend subsection 12B(6) to (8) by replacing the word 'organisations' with the term 'regulated entities'. This is required because of the broader range of entities that are being regulated under the Privacy Act, particularly under the new credit reporting provisions.

Item 42 Sections 13 and 13A

Item 42 will repeal sections 13 and 13A and replace them with a new section 13. The new section will outline the circumstances that will result in an 'interference with the privacy of an individual'. This is based on repealed sections 13 and 13A but is drafted to reflect the newly APPs and also cover additional breaches, such as a breach of a registered APP code.

Under subsection 13(1), an act or practice of an APP entity will be an interference with the privacy of an individual where it breaches an APP in relation to personal information about the individual, or breaches a registered APP code that binds the entity in relation to personal information about the individual.

Subsection 13(2) provides that an act or practice of an entity will be an interference with the privacy of an individual if it breaches a provision of Part IIIA (credit reporting) or it breaches the registered CR code in relation to personal information about the individual and the code binds the entity.

Subsection 13(3) provides that an act or practice of a contract service provider which is an organisation will be an interference with the privacy of an individual in certain circumstances. This is based on the repealed paragraph 13A(1)(c). It will apply where:

- the act or practice relates to personal information about the individual
- the act or practice does not breach the APPs, or a registered APP code that binds the organisation in relation to the personal information because of a provision of the contract that is inconsistent with the principle or code, and
- the act is done, or the practice is engaged in, in a manner contrary to, or inconsistent with, that provision.

Subsection 13(4) provides that an act or practice of a tax file number recipient will be an interference with the privacy of an individual if it breaches a rule issued under section 17 in relation to tax file number information that relates to the individual, or it involves an

unauthorised requirement or request for disclosure of the tax file number. This is based on the old paragraphs 13(b) and (c) of the Privacy Act.

Subsection 13(5) provides that an act or practice will be an interference with the privacy of an individual if it constitutes a breach of Part 2 of the *Data-matching Program (Assistance and Tax) Act 1990* or the rules issued under section 12 of that Act. It will also be an interference with the privacy of an individual if it constitutes a breach of the rules issued under section 135AA of the *National Health Act 1953*. This is based on the old paragraphs 13(ba) and (bb) of the Privacy Act.

The note at the foot of subsection 13(5) notes that there are other Acts that may provide that an act or practice is an interference with the privacy of an individual.

Item 43 Subsection 13B(1)

Item 43 will amend subsection 13B(1) by removing the reference to paragraphs 13A(1)(a) and (b) and replacing it with a reference to subsection 13(1). This will reflect an earlier amendment which repealed and replaced sections 13 and 13A.

Item 44 Subsection 13B(1)

Item 44 will amend subsection 13B(1) by rendering the words 'of an individual' in bold, italic type. This will indicate that those words form part of the newly defined term 'interference with the privacy of an individual'.

Item 45 Subsection 13B(2)

Item 45 will repeal and replace subsection 13B(2).

The new subsection 13B(2) will contain an updated indication of the newly defined term 'interference with the privacy of an individual'. It will also contain an updated reference to subsection 13(3), rather than paragraphs 13A(1)(c) or (d), which will reflect the amendments to sections 13 and 13A.

Item 46 Subsection 13C(1)

Item 46 will amend subsection 13C(1) by rendering the words 'of the individual' in bold, italic type. This will indicate that those words form part of the newly defined term 'interference with the privacy of an individual'.

Item 47 Subsection 13C(2)

Item 47 will repeal and replace subsection 13C(2). This will update the reference to section 13A by replacing it with a reference to the new subsections 13(1) and (3), which will reflect an earlier amendment which repealed and replaced sections 13 and 13A.

Item 48 Subsection 13D(1)

Item 48 will amend subsection 13D(1) by rendering the words 'of an individual' in bold, italic type. This will indicate that those words form part of the newly defined term 'interference with the privacy of an individual'.

Item 49 Subsection 13D(2)

Item 49 will repeal and replace subsection 13D(2).

This will update the reference to section 13A by replacing it with a reference to the new subsections 13(1) and (3), which will reflect an earlier amendment which repealed and replaced sections 13 and 13A.

Item 50 Sections 13E and 13F

Item 50 will repeal sections 13E and 13F and replace them with new sections 13E, 13F and 13G.

Section 13E

The new section 13E will contain an updated indication of the newly defined term 'interference with the privacy of an individual'. It will also contain an updated reference to subsections 13(2), (4) and (5), rather than all of section 13, which will reflect earlier amendments to section 13.

Section 13F

The new section 13F will contain an updated indication of the newly defined term 'interference with the privacy of an individual'. It will also remove the reference to section 13A, which was repealed by an earlier amendment.

Section 13G

Section 13G will implement the Government's response to ALRC Recommendation 50-2, by creating a civil penalty where an entity does an act or engages in a practice which is a serious interference with the privacy of an individual, or where the entity repeatedly does an act, or engages in a practice that is an interference with the privacy of one or more individuals.

The provision is supported by a later amendment which will introduce a new section 80W, allowing the Commissioner to apply to the Federal Court or Federal Magistrates Court where a civil penalty provision, such as section 13G, has been contravened.

Section 13G will not define what constitutes a 'serious' or 'repeated' interference with the privacy of an individual. The ordinary meaning of these words will apply.

For example, a serious interference could occur if a health services provider disregards the Privacy Act by, without consent, knowingly disclosing detailed and sensitive personal information about an individual directly to a marketing organisation, which uses that information to send direct marketing to the individual. The interference could be exacerbated if, for example, as the result of the marketing, the individual's health information is disclosed to his or her family members.

Conversely, where an entity suffers a data breach through, for example, hacking, which compromises the personal information of a large number of individuals, it may be that the entity has not committed an interference with the privacy of individuals if the entity had taken reasonable security precautions to prevent the breach (including taking steps to implement systems to prevent hacking).

However, if the entity has not taken reasonable precautions to prevent or minimise a breach, and a breach occurs, then it may be that the failure constitutes an interference with privacy. Depending on the circumstances, such a breach could be a 'serious' interference.

In addition to the above, it is anticipated that the OAIC will develop enforcement guidelines which will set out the criteria on which a decision to pursue a civil penalty will be made. These guidelines will assist in provide further clarity and context for the term.

Item 51 Section 17

Item 51 will repeal and replace section 17. This amendment is necessary because of changes made by the Legislative Instruments Act. It is not a policy change, but will amend the law to reflect the actual status of the rules.

Item 52 Section 18 (heading)

Item 52 will repeal and replace the heading to section 18.

This will remove the word 'guidelines' and replace it with the word 'rules'. This change in terminology will implement the Government's response to ALRC Recommendation 47-2. The word 'rule' will be used where appropriate throughout the Privacy Act to more accurately reflect the binding nature of certain guidelines and to distinguish binding instruments issued or approved by the Commissioner from voluntary guidance.

Item 53 Section 18

Item 53 will amend section 18 by removing the word 'guideline' and replacing it with the word 'rule'.

This change in terminology will implement the Government's response to ALRC Recommendation 47-2. The word 'rule' will be used where appropriate throughout the Privacy Act to more accurately reflect the binding nature of certain guidelines and to distinguish binding instruments issued or approved by the Commissioner from voluntary guidance.

Item 54 Sections 27 to 29

Item 54 will repeal and replace sections 27 to 29.

The provisions dealing with the functions and powers of the Commissioner will be consolidated and redrafted according to the overarching objective of achieving greater logical consistency, simplicity and clarity, which will go towards implementing the Government's response to ALRC Recommendation 5-2. Consolidation of the existing provisions will reduce repetition and assist in simplifying the Privacy Act.

The structure of the new sections will follow a compliance-oriented approach to regulatory design. The Commissioner's functions will be grouped according to whether they foster compliance (the guidance related functions), monitor compliance (the monitoring related functions) or support compliance (the advice related functions).

This amendment will also implement the Government's response to ALRC Recommendation 47-3, by removing the requirement in the current subsection 27(g) for the Commissioner to

maintain a Personal Information Digest. The new APP 1, which will be introduced by amendments made in Schedule 1, will provide an appropriate level of transparency as to how agencies handle personal information, as it is envisaged that entities will make privacy policies electronically available. This will reduce the compliance burden of maintaining a Personal Information Digest.

Section 27 Functions of the Commissioner

The new section 27 will deal with the functions of the Commissioner generally. Under subsection 27(1), the Commissioner will have functions conferred by the Privacy Act or any other law of the Commonwealth. For example, the Commissioner also has privacy responsibilities under the *Data-matching Program (Assistance and Tax) Act 1990*, the *National Health Act 1953*, the *Crimes Act 1914* and the *Telecommunications Act 1997*.

The Commissioner will also have the guidance related functions (section 28), the monitoring related functions (section 28A) and the advice related functions (section 28B).

The Commissioner will also have the function of doing anything incidental or conducive to the performance of any of the above functions, and the power to do all things necessary or convenient to be done for, or in connection with, the performance of the Commissioner's functions.

Subsection 27(3) will implement the Government's response to ALRC Recommendation 46-5 by providing that the Commissioner may establish expert panels to assist the Commissioner in performing any of its functions. While the OAIC already convenes expert panels, the ALRC considered that it would be advantageous to expressly set out that power in the Privacy Act. Among other things, expert panels may be used to advise on difficult and emerging areas of privacy regulation. These expert panels will be separate from the Privacy Advisory Committee dealt with in Part VII, and unlike that Committee, the Commissioner will have broad discretion about membership, functions and meetings of any expert panels established.

Subsection 27(4) provides that section 38 of the *Healthcare Identifiers Act 2010* (Healthcare Identifiers Act), rather than section 12B of the Privacy Act (which deals with severability), applies in relation to an investigation of an act or practice referred to in subsection 29(1) of that Act.

Section 38 of the Healthcare Identifiers Act is intended to ensure that the Healthcare Identifiers Act is given the widest possible operation consistent with Commonwealth constitutional legislative power. Subsection 38(1) provides that without limiting the effect of the Healthcare Identifiers Act, Parts 3 and 4 of that Act also have effect as provided by each of subsections 38(2) to 38(10) relying on different elements of Commonwealth power.

Section 28 Guidance related functions of the Commissioner

The new section 28 outlines the 'guidance related functions' of the Commissioner, mentioned in new paragraph 27(1)(b). This section will combine a number of the functions in the previous sections 27 and 28A of the Privacy Act. These functions are being combined and expressed to apply to entities as appropriate.

Under paragraph 28(1)(a), the 'guidance related functions' include making guidelines for the avoidance of acts or practices that may or might be interferences with the privacy of individuals, or which may otherwise have any adverse effects on the privacy of individuals. This is based on former paragraph 27(1)(e) and is intended to give the Commissioner a general function to provide information relating to avoiding any breaches of privacy. Pursuant to subsection 28(4) these guidelines are not a legislative instrument.

Under paragraph 28(1)(b), the 'guidance related functions' include making guidelines by legislative instrument about the disclosure of biometric information and templates by non-enforcement agencies under APP 6.3. This is an important safeguard for the application of that provision that ensures the Commissioner has an ongoing role in determining the appropriate rules for the disclosure of that type of information.

Under paragraph 28(1)(c), the 'guidance related functions' include promoting an understanding and acceptance of the APPs, the credit reporting provisions and the objects of those principles and provisions, and the registered APP and CR codes.

The function to undertake education programs (found in the previous paragraph 27(1)(m)) is retained in new paragraph 28(1)(d). Under subsection 28(3), these may be undertaken by either the Commissioner, or a person or authority acting on the Commissioner's behalf.

The Commissioner may publish the guidelines referred to under paragraphs 28(1)(a) and (b) in such manner as the Commissioner considers appropriate.

Section 28A Monitoring related functions of the Commissioner

The new section 28A will outline the monitoring related functions of the Commissioner, mentioned in the new paragraph 27(1)(c). Subsection 28A(1) outlines functions that are applicable to credit reporting and tax file number information and are based on functions in the former sections 28 and 28A of the Privacy Act.

Under subsection 28A(1), the 'monitoring related functions' include monitoring the security and accuracy of information held by entities regulated by Part IIIA (credit reporting). The Commissioner will also have the function of examining the records of entities to ensure that they are not using information to which the credit reporting provisions apply for unauthorised purposes, and are taking adequate measures to prevent the unlawful disclosure of such information. These functions are based on former paragraphs 28A(1)(h) and (j) of the Privacy Act.

In relation to tax file number information in new paragraphs 28A(1)(c) to (e), the Commissioner will have the power to examine the records of the Commissioner of Taxation (COT) to ensure that the COT is not using tax file number information for purposes beyond his or her powers, and is taking adequate measures to prevent the unlawful disclosure of such information. The Commissioner will also have the function of evaluating compliance with the rules issued under section 17, and monitoring the security and accuracy of tax file number information kept by file number recipients. These functions are based on former paragraphs 28(1)(d), (e) and (h) of the Privacy Act.

Under subsection 28A(2), the Commissioner has a range of general monitoring related functions which are based on functions in former paragraphs 27(1)(b), (c), (k) and (q). These include examining (on request by a Minister or Norfolk Island Minister, or on the

Commissioner's own initiative) proposed enactments or data-matching or linkage proposals to assess whether they may have adverse privacy implications, and ensuring that those impacts are minimised.

The Commissioner will also have the function of undertaking research and monitoring developments in data processing and technology to ensure that any adverse privacy implications are minimised, and reporting to the Minister about that research and development. Finally, the Commissioner will also retain the function of monitoring and reporting on the adequacy of equipment and user safeguards. The reporting in either of these instances, if completed in writing, is not a legislative instrument.

Under subsection (3), the Commissioner may exercise the functions in paragraphs 28A(2)(a) and (b) on the Commissioner's own initiative or on request by a Minister or Norfolk Island Ministers. All other functions conferred in subsections (1) and (2) may be exercised on the Commissioner's own initiative alone.

Section 28B Advice related functions of the Commissioner

The new section 28B will outline the 'advice related functions' of the Commissioner, mentioned in the new paragraph 27(1)(c). These are based on functions that were included in former paragraphs 27(1)(f), (j), (r) and 28(1)(g) of the Privacy Act.

Under paragraph 28B(1)(a) the Commissioner has the general advice related function of providing advice to a Minister, Norfolk Island Minister or entity about any matter relevant to the operation of this Privacy Act. This may be performed by the Commissioner on request or on the Commissioner's own initiative.

Paragraph 28B(1)(b) provides that the Commissioner has the general advice related function of informing the Minister of action that needs to be taken by an agency in order to comply with the APPs. Under subsection 28B(3), the Commissioner may perform this function whenever the Commissioners think it is necessary to do so. If the Minster is informed in writing, the instrument will not be a legislative instrument.

Paragraph 28B(1)(c) provides that the Commissioner has the general advice related function of providing reports and recommendations to the Minister in relation to any matter concerning the need for, or the desirability of, legislative or administrative action in the interests of the privacy of individuals. As with paragraph (1)(a), this may be performed by the Commissioner on request or on the Commissioner's own initiative. If the Minster is informed in writing, the instrument will not be a legislative instrument.

Paragraph 28B(1)(d) provides that the Commissioner has the general advice related function of providing advice to file number recipients about their obligations under the *Taxation Administration Act 1953* in relation to the confidentiality of tax file number information, or any matter relevant to the operation of that Act. This may be performed by the Commissioner on request or on the Commissioner's own initiative.

Subsection 28B(4) is included to assist readers, as the instrument is not a legislative instrument within the meaning of section 5 of the Legislative Instruments Act. This subsection will be declaratory of the law, rather than creating an exemption from that Act.

Section 29 Commissioner must have due regard to the objects of the Act

The new section 29 will require that in performing functions and exercising powers conferred by the Privacy Act, the Commissioner must have due regard to the objects of the Privacy Act, which were inserted by an earlier amendment. See new section 2A above. Former paragraphs 29(a) to (c) are largely covered by the content of the objects clause.

This amendment will implement the Government's response to Recommendation 46-3 of the ALRC that the Commissioner have regard to the new objects of the Privacy Act in undertaking functions and exercising his or her powers. This will ensure that matters that the Commissioner has regard to in the administration of the Privacy Act are in line with the objects by which the community interprets and applies the Privacy Act.

Item 55 Subparagraph 30(1)(b)(ii)

Item 55 will repeal and replace subparagraph 30(1)(b)(ii) which uses terminology more consistent with new conciliation powers of Commissioner which will be introduced by a later amendment.

Item 56 Subsection 30(3)

Item 56 will amend subsection 30(3) by removing the references to paragraphs 27(1)(a), 28(1)(b) and (c) and 28A(1)(b). These provisions are being repealed by virtue of other amendments in the Bill. The effect of this amendment is that the Commissioner must, in certain circumstances, report to the Minister about investigations about an act or practice of an agency, file number recipient, credit reporting body or credit provider that the Commissioner thinks is an interference with the privacy of an individual. Paragraphs 27(1)(a), 28(1)(b) and (c) and 28A(1)(b) are replaced with the similar 'interference with the privacy of an individual' concept below in item 57.

Item 57 Subsection 30(3)

Item 57 will amend subsection 30(3) by inserting a qualifier that the act or practice must be 'an interference with the privacy of an individual under subsection 13(1), (2) or (4)'. As noted above, this replaces the references to paragraphs 27(1)(a), 28(1)(b) and (c) and 28A(1)(b).

Item 58 Subsection 30(6)

Item 58 will repeal subsection 30(6). This subsection is unnecessary with the replacement of the existing subsection 40(1B). It is also clear from subsection 30(1) that the section does not apply to a complaint made under section 36.

Item 59 Subsection 31(1)

Item 59 will amend subsection 31(1) by removing the reference to paragraph 27(1)(b) and replacing it with a reference to paragraph 28A(2)(a).

This will reflect an earlier amendment which repealed and replaced sections 27 to 29. The content of the new paragraph 28A(2)(a) will largely replicate the content of former paragraph 27(1)(b).

Item 60 Subsection 31(2)

Item 60 will amend subsection 31(2) by removing the phrase 'agency or organisation' and replacing it with the word 'entity'.

This will reflect terminology changes which will be brought about by amendments in Schedule 1.

Item 61 Section 32 (heading)

Item 61 will repeal and replace the heading to section 32. The new heading is a more accurate description of the Commissioner's activities under the new section 32.

Item 62 Subsection 32(1)

Item 62 will repeal and replace subsection 32(1).

This will reflect an earlier amendment which repeals and replaced sections 27 to 29. The content of the new paragraphs and sections listed in the new subsection 32(1) will largely replicate the content of the former paragraphs listed in the repealed subsection 32(1). In particular, the listed audit functions will be consolidated in the Commissioner's new power to conduct an assessment under section 33C.

Item 63 Subsection 32(2)

Item 63 will amend subsection 32(2) by inserting the words 'or assessment' after the word 'activity'. This will reflect an earlier amendment which repealed and replaced subsection 32(1). The new subsection 32(1) refers to both activities and assessments.

Item 64 After section 33B

Item 64 will insert new Divisions 3A and 3B after section 33B.

Division 3A— Assessments by, or at the direction of, the Commissioner

Section 33C Commissioner may conduct an assessment relating to the Australian Privacy Principles etc.

The new section 33C will implement the Government's response to ALRC Recommendation 47-6, by empowering the Commissioner to conduct an assessment of an APP entity's maintenance of personal information. The assessment will be to determine whether personal information held by the entity is being maintained according to the APPs, credit reporting provisions and other specified relevant rules or codes (paragraphs 33C(1)(a), (b), (c), (d) and (e)). This will consolidate the Commissioner's existing discretions to conduct audits of agencies, file number recipients and credit reporting agencies and credit providers and extend the discretion to include organisations.

The power to conduct an assessment of whether information is being maintained in accordance with the provisions of Part IIIA is intended to extend to assessing whether that information is maintained in accordance with a particular APP, where Part IIIA specifies that the APP applies to credit-related information.

As noted by the ALRC, this discretion will allow the Commissioner to take a snapshot of the compliance levels in an agency or organisation or across an industry. Spot assessments can act as an important preventative measure by encouraging entities to take compliance with the Privacy Act seriously. The assessments are intended to be of an educational and non-confrontational nature, and to provide an avenue for the Commissioner to give one-on-one guidance to an entity without needing to resort to mandatory enforcement action.

The new section will not provide criteria for when an assessment could or should be conducted. It is intended that the discretion will be used consistently with the existing approach of the OAIC, including where agencies or organisations are undertaking actions or new ways of dealing with personal information which could impact on privacy.

Section 33D Commissioner may direct an agency to give a privacy impact assessment

The new section 33D will implement the Government's response to ALRC Recommendation 47-4, by empowering the Commissioner to:

- direct an agency to provide the Commissioner with a privacy impact assessment (subsection 33D(1)); and
- report to the responsible Ministers when an agency fails to comply with the direction (subsection 33D(6)).

This will be a discretionary power. It is expected that agencies will continue to voluntarily conduct privacy impact assessments as appropriate when developing policies which will impact on privacy, as part of their compliance with their obligations under the Privacy Act. It is not expected that the Commissioner will be aware of all new government proposals, and accordingly this power may be used when the Commissioner has been notified about a proposal by the agency or other sources. While the overall approach of the Privacy Act is to be technologically neutral, one use of a privacy impact assessment might be to assess the use of new technologies which may have significant impacts on privacy.

Subsection 33D(3) will include a definition of a 'privacy impact assessment' to mean a written assessment that identifies the impact an activity or function might have on the privacy of individuals and sets out recommendations for managing, minimising or eliminating that impact. Under subsection 33D(4), assessments are not limited to the elements in the definition, though, and can contain additional elements if desired.

The requirement in subsection 33D(7) to undertake a review of section 33D within five years of its commencement will partially implement the Government's response to ALRC Recommendation 47-5. The review will be to assess whether the Commissioner's power to direct that a privacy impact assessment be conducted should be extended to include organisations.

Subsections 33D(2) and (5) will be included to assist readers, as the directions and assessments are not legislative instruments within the meaning of section 5 of the Legislative Instruments Act. These subsections will be declaratory of the law, rather than creating an exemption from that Act.

Division 3B— Enforceable undertakings

The new sections 33E and 33F will implement the Government's response to ALRC Recommendation 50-4. That response noted that the ALRC recommendation aligned closely with the compliance-oriented approach of the Privacy Act as it would allow entities to take active responsibility for actions which might otherwise result in a court-based outcome. New sections 33E and 33F are based on a similar provision in Part 31A of the *Telecommunications Act 1997* which gives the Australian Communications and Media Authority the power to accept and enforce an undertaking.

Section 33E Commissioner may accept undertakings

New section 33E will empower the Commissioner to accept written undertakings by entities that they will take, or refrain from taking, specific action to ensure compliance with the Privacy Act or to ensure that, in the future, they do not do an act, or engage in a practice, that interferes with the privacy of an individual.

Under subsection 33E(1), the written undertaking given by the entity will relate to either: taking specified action; refraining from taking specified action; or taking specified action directed towards ensuring that the entity does not do an act, or engage in a practice in the future that interferes with the privacy of an individual. Under subsections 33E(2) and (3), the undertaking must be expressed to be an undertaking under section 33E, and can be withdrawn or varied at any time provided the Commissioner has consented. The Commissioner may also cancel the undertaking at any time with written notice.

Section 33F Enforcement of undertakings

New section 33F provides that, if the section 33E undertaking is breached (and it has not been withdrawn or cancelled) the Commissioner may apply to the Federal Court or the Federal Magistrates Court for an order directing the entity to comply with the undertaking, pay compensation, or any other order the court considers appropriate.

Item 65 Subsections 34(1) and (2)

Item 65 will amend subsections 34(1) and (2) by removing the phrase 'functions referred to in section 27' and replacing it with the term 'Commissioner's functions'.

This will reflect an earlier amendment which repealed and replaced section 27 and restructured the provisions relating to the Commissioner's functions.

Item 66 At the end of Part IV

Item 66 will insert a new section 35A at the end of Part IV which will give the Commissioner the power to recognise external dispute resolution schemes. This will partly implement the Government's response to Recommendation 49-2 to amend the Privacy Act to empower the Commissioner to decline to investigate a complaint where the complaint is being handled by an external dispute resolution scheme (EDR) recognised by the Commissioner. It is appropriate that the Commissioner should have the discretion to allow complaints to be dealt with by particular external dispute resolution schemes which the Commissioner deems can effectively deal with complaints.

New subsection 35A(1) gives the Commissioner the power to recognise an external dispute resolution scheme for an entity or a class of entities, or for a specified purpose. Subsection 35A(2) will list matters the Commissioner must take into account in considering whether to recognise a scheme. These are modelled on the matters which must be considered by the Australian Securities and Investments Commission when approving an external dispute resolution scheme under the Corporations Act, Corporations Regulations and National Credit Regulations.

Under subsection 35A(3), the Commissioner will have the power to specify a period of recognition for a particular scheme, and to make the recognition of a scheme subject to specified conditions. The Commissioner will also be empowered to vary or revoke a period of recognition, a specified condition, or the recognition of a scheme.

Subsection 35A(4) states that a notice under subsection (1) that a scheme is recognised is not a legislative instrument. This will be included to assist readers, as the notice is not a legislative instrument within the meaning of section 5 of the Legislative Instruments Act. This subsection will be declaratory of the law, rather than creating an exemption from that Act.

Item 67 Part V (heading)

Item 67 will repeal and replace the heading to Part V.

This will add the word 'etc.' to the end of the heading 'Investigations'. This will clarify that Part V deals with a greater range of matters than just the Commissioner's investigation powers and their consequences.

Item 68 Before Division 1 of Part V

Item 68 will insert a new Division 1A before Division 1 of Part V.

This new Division 1A will contain a guide to Part V, which will provide a brief outline to the contents of the Part. The outline contains details about complaint-handling and investigations.

Item 69 Subsection 36(7) (note)

Item 69 will amend the note to subsection 36(7) by replacing the reference to section 70A with a reference to sections 98A to 98C.

This will reflect later amendments which will repeal section 70A and insert new sections 98A to 98C dealing with the Privacy Act's treatment of partnerships, unincorporated associations and trusts.

Item 70 Subsection 36(8)

Item 70 will amend subsection 36(8) by removing the reference to paragraphs 13(b) to (d) and replacing it with a reference to subsections 13(2), (4) and (5).

This will reflect earlier amendments to section 13. The new subsections 13(2), (4) and (5) will deal with the same content as is currently dealt with by paragraphs 13(b) to (d).

Item 71 Subsection 36(8)

Item 71 will amend subsection 36(8) by inserting a reference to an entity in addition to the existing reference to a person. This is more consistent with the terminology and the entities regulated under the new regime in the Privacy Act.

Item 72 Subsection 38(1)

Item 72 will amend subsection 38(1) by removing the reference to representative complaints being accepted under subsection 40(1B). This will reflect a later amendment which will repeal and replace subsection 40(1B).

Item 73 Paragraph 38(1)(a)

Item 73 will amend paragraph 38(1)(a) by inserting a reference to an entity in addition to the existing reference to a person. This is more consistent with the terminology and the entities regulated under the new regime in the Privacy Act.

Item 74 Subsection 38(2)

Item 74 will amend subsection 38(2) by removing the reference to representative complaints being accepted under subsection 40(1B). This will reflect a later amendment which will repeal and replace subsection 40(1B).

Item 75 Subsection 38B(2)

Item 75 will amend subsection 38B(2) by removing the end of the subsection and replacing it with two paragraphs.

The new paragraph 38B(2)(a) will implement the Government's response to ALRC Recommendation 49-9, by providing that a class member may withdraw from a representative complaint at any time if the complaint was lodged without the member's consent. Currently, subsection 38(3) allows a representative complaint to be lodged without the consent of class members, and section 39 prevents class members of a representative complaint from lodging individual complaints in respect of the same subject matter. This amendment is intended to eliminate the possibility that a person's capacity to make an individual complaint could be removed when he or she has become a class member of a representative complaint lodged without his or her consent. Where a person does withdraw from a representative complaint under paragraph 38B(2)(a), he or she will not be prohibited from lodging an individual complaint.

The new paragraph 38B(2)(b) will simply maintain the current content of the subsection. That is, the withdrawal from the representative complaint may come at any time before the Commissioner begins to hold an inquiry.

Item 76 Add at the end of subsection 38B(2)

Item 76 will add a note at the end of subsection 38B(2).

The note will make clear that a class member who withdraws from a representative complaint may then go on to make an individual complaint under section 36 in relation to the same

matter as the representative complaint. This will express the intention of an earlier amendment to subsection 38B(2).

Item 77 Subsections 40(1B) and (1C)

Item 77 will repeal and replace subsections 40(1B) and (1C).

Subsection 40(1B) will be repealed because privacy codes will no longer contain alternative complaint mechanisms, rendering the subsection unnecessary.

New subsection 40(1B) provides that subsection 40 (1A) does not apply to certain complaints. Subsection 40(1A) provides that the Commissioner must not investigate a complaint under section 36 if the complainant did not complain to the respondent before making the complaint to the Commissioner (unless the Commissioner believes it was not appropriate for the complainant to complain to the respondent). This amendment allows the Commissioner to investigate a complaint made first to the Commissioner, where it relates to certain credit reporting provisions (e.g. concerning access and correction) or a provision of a registered code that relates to those provisions.

Item 78 Subsection 40(2)

Item 78 will amend subsection 40(2) by inserting the phrase, 'on the Commissioner's own initiative', in relation to the Commissioner's investigation under that subsection of acts or practices.

This will create consistency of terminology with the FOI Act in relation to Commissioner initiated investigations.

Item 79 Paragraph 40(2)(a)

Item 79 will amend paragraph 40(2)(a) by adding a breach of APP 1 to the circumstances in which the Commissioner may investigate an act or practice on his or her own initiative.

This amendment will enable the Commissioner to initiate an investigation without a complaint into a possible breach of APP 1. That APP is concerned with open and transparent management of personal information, including through the development of enhanced and accessible privacy policies. A breach of that principle may not necessarily result in the breach of the privacy of an individual. For example, an entity may contravene the principle if it fails to have an up-to-date APP privacy policy about the management of personal information by the entity, because it has not updated in for a period of time. While that is unlikely to be a breach of the privacy of an individual, it is still potentially a breach of APP 1. To encourage compliance, it is important for the Commissioner to be able to initiate an investigation into any possible breach. Individuals who are not directly adversely affected by a breach of APP 1 should not be able to make a complaint.

Item 80 Section 40A

Item 80 will repeal and replace section 40A.

The current section 40A deals with complaints made to an adjudicator for an approved privacy code. Because privacy codes will no longer contain alternative complaint

mechanisms and code adjudicators will no longer exist in the amended Privacy Act, this section will no longer be necessary.

The new section 40A will deal with the conciliation of complaints and will partially implement the Government's response to ALRC Recommendation 49-5. It will provide that if the Commissioner considers it reasonably possible that a complaint made under section 36 may be successfully conciliated, the Commissioner must make a reasonable attempt to conciliate the complaint. This will not apply if the Commissioner has decided under section 41 or 50 not to investigate further, the act or practice.

If the Commissioner is satisfied that there is no reasonable likelihood that the complaint will be successfully conciliated, the Commissioner must notify the complainant and respondent in writing, and will then have to decide whether to investigate the complaint further, or not. The parties to a failed conciliation will not have the power to compel the Commissioner to make a determination.

Importantly, subsection 40A(5) will provide that evidence of anything said or done during conciliation cannot be used in any hearing before the Commissioner, or in any legal proceedings, relating to the complaint or the act or practice, without the consent of the complainant and respondent. However, the evidence will be admissible if the thing was said or done in furtherance of the commission of a fraud or offence, or the commission of an act that renders a person liable to a civil penalty.

Item 81 Section 41 (heading)

Item 81 will repeal and replace the heading to section 41.

The new heading will include the phrase 'may or must'. This will reflect a later amendment which will introduce a requirement that the Commissioner must not investigate or investigate further if a complainant has withdrawn the complaint.

Item 82 Subsection 41(1)

Item 82 will amend subsection 41(1) by removing the reference to complaints being accepted under subsection 40(1B). This will reflect an earlier amendment which repealed and replaced subsection 40(1B).

Item 83 At the end of paragraphs 41(1)(a) and (c)

Item 83 will add the word 'or' to the end of paragraphs 41(1)(a) and (c). This is a drafting update to make it clear that each paragraph in subsection 41(1) is a separate ground for the Commissioner to decline to investigate a complaint made under section 36.

Item 84 Paragraph 41(1)(d)

Item 84 will amend paragraph 41(1)(d) by adding the situation where a complaint was not made in good faith to the list of circumstances where the Commissioner may decide not to investigate an act or practice.

This will make paragraph 41(1)(d) consistent with the new subsection 73(1A), which will provide that the Commissioner may dismiss an APP entity's application for a public interest determination if the Commissioner is satisfied that the application is not made in good faith.

It will also create consistency with section 54W of the FOI Act, which gives the Commissioner the power to decide not to undertake or continue an IC review if the application is not made in good faith.

Item 85 After paragraph 41(1)(d)

Item 85 will insert additional situations into the list of circumstances where the Commissioner may decide not to investigate an act or practice.

Paragraph 41(1)(da) will implement the Government's response to ALRC Recommendation 49-1(c) by providing that the Commissioner may decide not to investigate an act or practice if the Commissioner is satisfied that, having regard to all the circumstances, an investigation or further investigation is not warranted. This will give the Commissioner greater flexibility to decline to investigate a complaint where it would be an unproductive or inefficient use of the Commissioner's powers.

In exercising this power, it is expected that the Commissioner will:

- apply the principles of administrative law
- outline, as appropriate, in the annual report, examples of where the power is used, and
- provide guidance as to the kinds of matters it would decline to investigate.

Paragraph 41(1)(db) will implement the Government's response to ALRC Recommendation 49-1(b) by providing that the Commissioner may decide not to investigate an act or practice if the Commissioner is satisfied that the complainant has not responded to a request from the Commissioner for information relating to the complaint. The Commissioner will be required to specify a time period within which the response must be provided, and wait until the period has expired, before making a decision not to investigate.

Paragraphs 41(1)(dc) and (dd) will implement the Government's response to ALRC Recommendation 49-2 by providing that the Commissioner may decide not to investigate an act or practice if the Commissioner is satisfied that:

- it is being dealt with by a recognised external dispute resolution scheme, or
- it would be more effectively or appropriately dealt with by a recognised external dispute resolution scheme.

An example of the latter may be where privacy is only a minor aspect of the complaint. This will allow the Commissioner to recognise the privacy mandates of external dispute resolution schemes that are not established under a legislative scheme (eg the Financial Services Ombudsman).

Item 86 After subsection 41(1)

Item 86 will amend section 41 by inserting a new subsection 41(1A).

This will implement the Government's response to ALRC Recommendation 49-1(a) by providing that the Commissioner must not investigate an act or practice if the complainant has withdrawn the complaint. It is considered that in those cases, an investigation would be an unproductive or ineffective use of the Commissioner's powers, and it is more appropriate

to require the Commissioner not to investigate rather than to provide a discretion to continue to investigate.

If the complaint raises matters which, in the opinion of the Commissioner, warrant investigation, the Commissioner will still have the discretion to launch an investigation on his or her own initiative under subsection 40(2).

Item 87 Subsections 41(2) and (3)

Item 87 will amend subsections 41(2) and (3) by removing the reference to complaints being accepted under subsection 40(1B). This will reflect an earlier amendment which repealed and replaced subsection 40(1B).

Item 88 Section 42

Item 88 will add a subsection number (1) to the beginning of the current contents of section 42. This will reflect the addition of a new subsection 42(2) in item 91 below.

Item 89 Section 42

Item 89 will amend section 42 by removing the reference to complaints being accepted under subsection 40(1B). This will reflect an earlier amendment which repealed and replaced subsection 40(1B).

Item 90 Section 42

Item 90 will add the words 'or any other person' to the end of section 42.

This will implement the first part of ALRC Recommendation 49-10, by extending the Commissioner's power to make inquiries of persons other than the respondent to a complaint. This section applies to preliminary inquiries made for the purpose of determining whether to investigate a complaint, or whether the Commissioner has the power to investigate the complaint. It is intended that the Commissioner will only use this power when making inquiries of third parties will result in more timely and efficient complaint resolution.

The latter part of ALRC Recommendation 49-10 suggested that the Commissioner be required to inform the complainant that inquiries of a third party will be made. However, the Commissioner will be required by APP 5 to notify individuals of the purposes for which personal information will be collected. This will require the Commissioner, when collecting information from a complainant, to notify them that the information may be used to make preliminary inquiries of third parties. An express requirement as recommended by the ALRC will therefore be unnecessary.

Item 91 At the end of section 42

Item 91 will add a new subsection 42(2) to the end of section 42.

This will give the Commissioner the power to make inquiries of any person in determining whether to investigate an act or practice on the Commissioner's own initiative under subsection 40(2). This will allow the Commissioner to make inquiries in order to determine whether the matter falls within the jurisdiction of the Privacy Act, before commencing an investigation.

Item 92 After subsection 43(1)

Item 92 will add a new subsection 43(1AA) into section 43.

This will provide that the Commissioner must inform the relevant person or entity of an investigation into its act or practice before commencing that investigation. This is a new requirement ensuring that the person or entity is given appropriate notice before a formal Commissioner initiated investigation is about to be undertaken. It will give that person and entity sufficient notice to begin gathering necessary information about the subject of the investigation, and an early opportunity to cooperate with the Commissioner.

Item 93 Subsection 43(2)

Item 93 will amend subsection 43(2) by removing the words 'in private but otherwise'.

Subsection 43(2) will then simply provide that an investigation under Part V, Division 1 shall be conducted in such a manner as the Commissioner thinks fit. The provision as it currently exists is unclear. This amendment will clarify that the Commissioner has the discretion to conduct investigations in public or private. It is important that this flexibility is available to the Commissioner to enable him or her to undertake the investigation in the most efficient way possible. It is also desirable to move from a default position of private investigations to enhance the Government's ongoing transparency and open government reforms.

Item 94 Subsections 43(4), (5) and (6)

Item 94 will repeal subsections 43(4), (5) and (6) and replace them with a new subsection 43(4).

This will remove the requirement that the Commissioner must afford the parties an opportunity to appear and make submission, orally, in writing or both before making a finding under section 52 that is adverse to a complainant or respondent. Instead, the Commissioner will be allowed to make a determination under that section without holding a hearing if all the listed circumstances are fulfilled.

This will go to implementing the Government's response to ALRC Recommendation 49-13, and will give the Commissioner greater discretion as to whether parties should be given an opportunity to make oral submissions prior to a decision being made. The amendment is intended to streamline the determination process where it is fair to do so.

The new subsection 43(4) will be modelled on subsection 55(1) of the FOI Act. This will facilitate more consistent procedures across the OAIC.

Removing subsection 43(5) will remove the requirement that the Commissioner afford an affected complainant, respondent, person or entity an opportunity to appear before the Commissioner if an adverse finding is to be made under section 52. However, the new paragraph 96(1)(c) will provide that any determination made by the Commissioner under subsection 52(1) or (1A) could be subject to merits review. The new section 43A will also include a safeguard that enables parties to apply for a hearing.

Item 95 Subsection 43(7)

Item 95 will amend subsection 43(7) by removing the reference to subsection 43(5) and replacing it with a reference to the Commissioner holding a hearing. This will reflect an earlier amendment which repealed subsection 43(5) (item 94 above).

Item 96 Subsection 43(8A)

Item 96 will amend subsection 43(8A) by removing the references to an approved privacy code and the NPPs and replacing them with references to the APPs and a registered APP code.

This will reflect amendments made in Schedule 1 which repeal the NPPs and IPPs and enact the APPs and registered APP codes.

Item 97 After section 43

Item 97 will insert a new section 43A after section 43.

This new section will provide that an interested party may apply to the Commissioner requesting that the Commissioner hold a hearing before making a determination under section 52 in relation to an investigation. The section will define who is an 'interested party' and set out steps the Commissioner must take when an application is made.

The new section will result from an earlier amendment which will remove the requirement that the Commissioner afford an affected complainant, respondent, person or entity an opportunity to appear before the Commissioner if an adverse finding is to be made under section 52.

The new section 43A will be modelled on section 55B of the FOI Act. This will facilitate more consistent procedures across the OAIC.

Item 98 Subsection 44(4)

Item 98 will amend subsection 44(4) by removing the reference to section 69. This will mean that section 44 is subject to section 70 only. This will reflect a later amendment which will repeal section 69.

Item 99 Subsection 46(1)

Item 99 will amend subsection 46(1) by removing NPP complaints and complaints accepted under subsection 40(1B) as exceptions to the section.

The removal of NPP complaints will reflect changes brought about by amendments in Schedule 1, whereby the NPPs will be repealed and replaced by the APPs. It will also implement ALRC Recommendation 49-11, by removing the limitation and allowing the Commissioner to exercise the power to direct attendance at a compulsory conference in relation to any complaint received.

The removal of subsection 40(1B) complaints will reflect an earlier amendment which repealed and replaced subsection 40(1B).

Item 100 Subsection 50(1)

Item 100 will amend subsection 50(1) by inserting a definition of 'alternative complaint body'.

This will be an exhaustive list of bodies to which the Commissioner may transfer certain complaints if the Commissioner forms the opinion that a complaint could have been made to one of those bodies and that the matter could be more conveniently or effectively dealt with by that body.

The list will include recognised external dispute resolution schemes. This complements the implementation of the Government's response to ALRC Recommendation 49-2, which was implemented by an earlier amendment giving the Commissioner the power to decline to investigate a complaint where the Commissioner considers it would be better dealt with by an external dispute resolution scheme.

Item 101 At the end of paragraph 50(2)(a)

Item 101 will amend paragraph 50(2)(a) by adding a new subparagraph 50(2)(a)(v).

This will include a recognised external dispute resolution scheme in the list of bodies to which the Commissioner may consider a complaint could have been made. This will be consistent with the inclusion of external dispute resolution schemes in the new definition of 'alternative complaint body' (item 100 above).

Item 102 Subsection 50(2)

Item 102 will amend subsection 50(2) by removing the list of bodies and replacing it with the newly defined term 'alternative complaint body'. This drafting approach simplifies and adds more clarity to section 50.

Item 103 Paragraphs 50(2)(c) and (e)

Item 103 will amend paragraphs 50(2)(c) and (e) by removing the list of bodies and replacing it with the newly defined term 'alternative complaint body'. This drafting approach simplifies and adds more clarity to section 50.

Item 104 At the end of paragraph 50(3)(a)

Item 104 will amend paragraph 50(3)(a) by adding a new subparagraph 50(3)(a)(v).

This will include a recognised external dispute resolution scheme in the list of bodies to which complaints referred under subsection 50(2) may be taken to be complaints made to those bodies.

Item 105 Subsection 50A(2) (note 2)

Item 105 will repeal and replace note 2 to subsection 50A(2).

The new note will more accurately describe the operation of subsection 53B(1) of the Privacy Act, which is being amended to include reference to a determination under the amended section 52.

Item 106 Subparagraph 51(1)(b)(i)

Item 106 will replace references to 'should' with 'must' in subparagraph 51(1)(b)(i) of the Privacy Act. This mandatory type language is consistent with the thrust of the Government's response to ALRC Recommendation 50-1 that a determination should include a requirement to take specified action within a specified period for the purpose of ensuring compliance with the Privacy Act. A consequence of failing to comply with the determination could mean that the determination is enforced in the Federal Court or Federal Magistrates Court.

Item 107 After subparagraph 52(1)(b)(i)

Item 107 will amend paragraph 52(1)(b) by adding a new subparagraph 52(1)(b)(ia).

This will implement the Government's response to ALRC Recommendation 49-6, by giving the Commissioner the power to make a declaration in relation to a substantiated complaint that the respondent must take specified steps to ensure that the conduct complained of is not repeated or continued. This will provide the Commissioner with an avenue to address systemic issues which may be raised by an individual's complaint and to direct the steps which should be taken to ensure future compliance with the Privacy Act.

A later amendment will provide that the specified steps must be reasonable and appropriate in the circumstances.

Item 108 Subparagraph 52(1)(b)(ii)

Item 108 will replace the reference to 'should' with 'must' in subparagraph 51(1)(b)(ii) of the Privacy Act. This mandatory type language is consistent with the thrust of the Government's response to ALRC Recommendation 50-1 that a determination should include a requirement to take specified action within a specified period for the purpose of ensuring compliance with the Privacy Act. A consequence of failing to comply with the determination could mean that the determination is enforced in the Federal Court or Federal Magistrates Court.

Item 109 Subsection 52(1A)

Item 109 will repeal subsection 52(1A) and replace it with new subsections 52(1A), (1AA) and (1AB).

The new subsection 52(1A) will outline the options open to the Commissioner after investigating an act or practice of a person or entity on the Commissioner's own initiative under subsection 40(2). These will largely replicate the options open to the Commissioner in relation to a substantiated complaint under subsection 52(1).

The determinations under subsection 52(1A) may include declarations that:

- the act or practice is an interference with the privacy of one or more individuals and the person or entity must not repeat or continue the act or practice
- the person or entity must take specified steps (provided they are reasonable and appropriate) within a specified period to ensure that the act or practice is not repeated or continued
- the person or entity must perform any reasonable act or course of conduct to redress any loss or damage suffered by one or more of those individuals

- one or more of those individuals are entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice, and
- it would be inappropriate for any further action to be taken in the matter.

The new subsection 52(1AB) will reflect the content of the repealed subsection 52(1A). That is, the loss or damage referred to in paragraph 52(1)(b) or subsection 52(1A) includes injury to the feelings of, and humiliation suffered by, the complainant or individual.

Item 110 Subsection 52(1B)

Item 110 will amend subsection 52(1B) by inserting a reference to subsection 52(1A) alongside the reference to subsection 52(1). Subsection 52(1B) provides that determinations are not binding or conclusive between any of the parties to the determination. The amendment will ensure that subsection 52(1B) operates so that a determination made under the amended subsection 52(1A) will be treated the same way as determinations made under the existing subsection 52(1).

Item 111 Subsections 52(3A) and (3B)

Item 111 will repeal subsections 52(3A) and (3B) and replace them with a new subsection 52(3A).

The current subsections 52(3A) and (3B) will be repealed because they do not appear to be necessary; they simply state a kind of order that the Commissioner may choose to make in some circumstances.

The Commissioner's general power to make orders is currently implied.

The new subsection 52(3A) will expressly provide a general power to allow the Commissioner to include in a determination under paragraph 52(1)(b) or subsection 52(1A) any order that he or she considers necessary or appropriate. This will make clear that the Commissioner has this power.

This amendment will also remove the references in the current subsection 52(3A) to the IPPs and NPPs, which will be repealed by amendments in Schedule 1 and replaced by the APPs and registered APP codes.

Item 112 Subsection 53A(1)

Item 112 will amend subsection 53A(1) by removing the phrase, 'to which a contracted service provider for a Commonwealth contract is the respondent', and replacing it with the phrase, 'that applies in relation to a contracted service provider for a Commonwealth contract'. That will make subsection 53A(1) more consistent with the terminology used in the amended section 52.

Item 113 Section 53B (heading)

Item 113 will repeal the heading to section 53B, 'Substituting respondent to determination', and replace it with, 'Substituting an agency for a contracted service provider'. This is a more accurate description of the operation of and the terminology used in section 53B.

Item 114 Paragraph 53B(1)(a)

Item 114 will repeal and replace paragraph 53B(1)(a). The replacement paragraph is more accurate and consistent with the terminology used in the amended section 52.

Item 115 After subparagraph 53B(1)(b)(i)

Item 115 will amend paragraph 53B(1)(b) by inserting a new subparagraph 53B(1)(b)(ia). This will reflect the earlier amendments to subsection 52(1A).

The new subparagraph 53B(1)(b)(ia) will include a reference to paragraph 52(1A)(d), which deals with declarations that an individual is entitled to compensation for loss and damage. In the same way, the existing subparagraph 53B(1)(b)(i) includes a reference to subparagraph 52(1)(b)(iii), which also deals with declarations that a complainant is entitled to compensation for loss or damage. The inclusion of the new subparagraph 53B(1)(b)(ia) will therefore create consistency.

Item 116 Paragraph 53B(1)(c)

Item 116 will amend paragraph 53B(1)(c) by removing the word 'respondent' and replacing it with the word 'provider'. This will maintain consistency of terminology with an earlier amendment to paragraph 53B(1)(a).

Item 117 Paragraph 53B(1)(d)

Item 117 will amend paragraph 53B(1)(d) by inserting the words 'or individuals' after the word 'complainant'. This will reflect an earlier amendment which incorporated determinations relating to individuals into paragraph 53B(1)(b).

Item 118 Paragraph 53B(1)(d)

Item 118 will amend paragraph 53B(1)(d) by removing the reference to subparagraphs 53B(1)(b)(i) and (b)(ii) and replacing it with a reference to paragraph 53B(1)(b). The individual specific references are unnecessary, as each subparagraph in paragraph 53B(1)(b) will refer to an amount of money.

Item 119 Subsection 53B(2)

Item 119 will amend subsection 53B(2) by rephrasing the subsection to make it more consistent with the terminology used elsewhere in section 53B. That involves removing references to 'the respondent to the determination'.

Item 120 Subsection 53B(2)

Item 120 follows on from item 119 in amending subsection 53B(2) by removing words in order to allow for the rephrasing inserted by item 119. The practical effect is the same in that the reference to the 'respondent' is a reference to the contracted service provider.

Item 121 Subsection 53B(2) (at the end of the note)

Item 121 will amend the note to subsection 53B(2) by inserting the words 'or individuals' after the word 'complainant' at the end of the note. This will reflect an earlier amendment which incorporated determinations relating to individuals into paragraph 53B(1)(b).

Item 122 Subsection 54(1)

Item 122 will amend subsection 54(1) by removing the phrase 'respondent to the determination is' and replacing it with the phrase 'determination applies in relation to'. This will maintain consistency with the changes in terminology made to section 53B.

Item 123 Section 55

Item 123 will repeal and replace section 55. This will extend the operation of the previous section 55 in two ways. Firstly, the section expressly refers to small business operators, who may be regulated by certain provisions of the Privacy Act (eg credit reporting provisions in Part IIIA of the Privacy Act as amended by Schedule 2 of the Bill). Secondly, it will also include the declarations made under the new subsection 52(1A) (which provides for a determination to be made following a Commissioner initiated investigation), such that organisations and small businesses will be required to comply with obligations referred to in those declarations.

Item 124 Subsection 55A(1)

Item 124 will amend subsection 55A(1) by removing the words 'any of' from the beginning of the subsection. This is a minor drafting change to remove redundant wording and is not a substantive amendment.

Item 125 Paragraphs 55A(1)(a) to (c)

Item 125 will amend subsection 55A(1) by repealing paragraphs 55A(1)(a) to (c) and replacing them with new paragraphs 55A(1)(a) and (b).

The new paragraph 55A(1)(a) will allow the complainant to commence proceedings to enforce a determination if the determination was made under subsection 52(1). The new paragraph 55A(1)(b) will allow the Commissioner to commence proceedings to enforce any determination to which the Division applies. That is consistent with the Government response to Recommendation 50-1 that the Commissioner should be able to enforce determinations made after Commissioner initiated investigations, in addition to determinations made under subsection 52(1).

Former paragraph 55A(1)(c) is being removed because privacy codes will no longer contain alternative complaint mechanisms and code adjudicators will no longer exist in the amended Privacy Act.

Item 126 Subsection 55A(2)

Item 126 will amend subsection 55A(2) by removing the word 'respondent' and replacing it with the phrase 'person or entity in relation to which the determination applies'. This change

in terminology is used for consistency with other amended sections that use ‘person or entity’, rather than ‘respondent’.

Item 127 Subsection 55A(2)

Item 127 will amend subsection 55A(2) by removing the term ‘the complainant’ and replacing it with the term ‘an individual’. This will make subsection 55A(2) more consistent with the concept of an ‘interference with the privacy of an individual’.

Item 128 Subsection 55A(5)

Item 128 will amend subsection 55A(5) by removing the word ‘respondent’ and replacing it with the phrase ‘person or entity in relation to which the determination applies’. This change in terminology is used for consistency with other amended sections that use ‘person or entity’, rather than ‘respondent’.

Item 129 Subsection 55A(5)

Item 129 will amend subsection 55A(5) by removing the term ‘the complainant’ and replacing it with the term ‘an individual’. This will make subsection 55A(5) more consistent with the concept of an ‘interference with the privacy of an individual’.

Item 130 Paragraph 55A(6)(c)

Item 130 will amend paragraph 55A(6)(c) by removing the word ‘appearance’ and replacing it with the word ‘hearing’.

This will reflect an earlier amendment which repealed subsections 43(4) to (6) and replaced them with a new subsection 43(4). The new subsection uses the word ‘hearing’ and no longer refers to appearances before the Commissioner.

Item 131 Paragraph 55A(6)(c)

Item 131 will amend paragraph 55A(6)(c) by removing the reference to subsection 43(5). This will reflect an earlier amendment which repealed subsection 43(5).

Item 132 Subsection 55A(7A)

Item 132 will amend subsection 55A(7A) by removing the phrase ‘matters that paragraph 29(a) requires the Commissioner to have due regard to’ and replacing it with the phrase ‘objects of this Act’.

This will reflect earlier amendments which inserted an objects clause as section 2A and repealed and replaced section 29 (items 1 and 54 above). The content of the objects clause is wider than that of the current paragraph 29(a), so this amendment will expand the range of matters the Court must have regard to under subsection 55A(7A).

Item 133 Paragraphs 55B(1)(a) and (b) and (3)(a) and (b)

Item 133 will repeal and replace paragraphs 55B(1)(a) and (b) and paragraphs 55B(3)(a) and (b).

This will remove the references in the current paragraphs to the IPPs and NPPs, which will be repealed by amendments in Schedule 1 and replaced by the APPs and registered APP codes. The new paragraphs will be consistent with the Schedule 1 amendments by referring to the APPs, APP entities and registered APP codes.

Item 134 Subsection 57(1)

Item 134 will amend subsection 57(1) by removing the phrase, 'has an agency, or the principal executive of an agency, as the respondent', and replacing it with the phrase, 'that applies in relation to an agency or the principal executive of an agency'.

This change in terminology is used for consistency with other amended sections that remove references to the 'respondent', and includes references to a determination 'that applies to ...' etc. This approach clarifies the entities or persons to which the subject determination applies.

Item 135 Section 58

Item 135 will repeal and replace section 58. This will extend the operation of the previous section 58 by expressly including reference to declarations made under the new subsection 52(1A), such that agencies will be required to comply with obligations referred to in those declarations.

Item 136 Section 59

Item 136 will amend section 59 by rephrasing part of the section. This change in terminology is used for consistency with other amended sections that remove references to the 'respondent', and includes references to a determination 'that applies to ...' etc. This approach clarifies the entities or persons to which the subject determination applies.

Item 137 Paragraph 59(b)

Item 137 will amend paragraph 59(b) by inserting a reference to paragraph 52(1A)(a) following the reference to subparagraph 52(1)(b)(i). This will reflect an earlier amendment to subsection 52(1A) that included a similar declaration to that in subparagraph 52(1)(b)(i), but which applies in the case of a Commissioner initiated investigation.

Item 138 After paragraph 59(b)

Item 138 will amend section 59 by inserting a new paragraph 59(ba).

This new paragraph will reflect earlier amendments which included a new subparagraph 52(1)(b)(ia) and a new paragraph 52(1A)(b). These are references to the new declarations that have been included in sections 51 and 52 that require a person or entity to take specified steps within a specified period to ensure that an act or practice is not repeated or continued. These will apply to a determination that applies in relation to the principal executive of an agency.

Item 139 At the end of paragraph 59(c)

Item 139 will amend paragraph 59(c) by inserting a reference to paragraph 52(1A)(c) following the reference to subparagraph 52(1)(b)(ii). This will reflect an earlier amendment

to subsection 52(1A) which introduces a similar determination power for the Commissioner after a Commissioner initiated inquiry.

Item 140 Subsection 60(1)

Item 140 will amend subsection 60(1) by inserting a reference to paragraph 52(1A)(d) following the reference to subparagraph 52(1)(b)(iii). This will reflect an earlier amendment to subsection 52(1A) which introduces a similar determination power for the Commissioner after a Commissioner initiated inquiry.

Item 141 Subsection 60(1)

Item 141 will amend subsection 60(1) by inserting the words 'or individual' after the word 'complainant'. This will reflect earlier amendments in, and make terminology consistent with, the new subsection 52(1A) which includes determinations relating to individuals.

Item 142 Subsection 60(2)

Item 142 will amend subsection 60(2) by removing the words 'respondent is' and replacing them with the phrase 'determination applies in relation to'. This change in terminology is used for consistency with other amended sections that remove references to the 'respondent', and includes references to a determination that 'applies in relation to' etc. This approach adds more clarity by specifying the entity or individual to which the determination will be applicable.

Item 143 Subsection 60(2)

Item 143 will amend subsection 60(2) by inserting the words 'or individual' after each instance of the word 'complainant'. This will reflect earlier amendments in, and make terminology consistent with, the new subsection 52(1A) which includes determinations relating to individuals.

Item 144 Section 61

Item 144 will repeal section 61. This will reflect a later amendment which will insert a new section 96 dealing with merits review by the Administrative Appeals Tribunal (AAT).

Item 145 Subsection 62(3)

Item 145 will repeal and replace subsection 62(3). The new paragraph 62(3)(a) will allow the complainant to apply for an order directing compliance only if the determination was made under subsection 52(1). The new paragraph 62(3)(b) will allow the Commissioner to apply for an order directing compliance with any determination to which the Division applies. This is consistent with the approach taken in the new section 55A, that the Commissioner should be able to enforce determinations made after Commissioner initiated investigations, in addition to determinations made under subsection 52(1).

Item 146 Subsection 62(4)

Item 146 will amend subsection 62(4) by removing the word 'respondent' and replacing it with the words 'agency or principal executive'. This change in terminology is used for consistency with other amended sections that remove references to the 'respondent'. This

approach clarifies the entity or individual to which the order under subsection 62(4) will be applicable.

Item 147 Paragraph 62(5)(a)

Item 147 will amend paragraph 62(5)(a) by removing the reference to section 61 and replacing it with a reference to section 96. This will reflect other amendments which repeal section 61 and insert a new section 96 dealing with the same subject matter.

Item 148 At the end of section 62

Item 148 will amend section 62 by adding a new subsection 62(6) which will define the term 'complainant' for the purposes of that section. This will be necessary because the former subsection 62(3), which included a very similar provision, will be repealed and replaced by an earlier amendment noted above in item 145.

Item 149 Subsection 63(2A)

Item 149 will amend subsection 63(2A) by removing the term 'NPP' and replacing it with the term 'APP'. This will remove the reference to 'the NPPs', which will be repealed by amendments in Schedule 1 and replaced by the APPs.

Item 150 Paragraphs 67(aa) and (ab)

Item 150 will repeal paragraphs 67(aa) and (ab).

Repealing paragraph 67(aa) will remove the reference to making complaints under an approved privacy code. This will reflect other amendments which replace approved privacy codes with registered APP codes, which do not contain alternative complaint mechanisms.

Repealing paragraph 67(ab) will remove the reference to accepting complaints under subsection 40(1B). This will reflect an earlier amendment which repealed and replaced subsection 40(1B). The existing subsection 40(1B) also deals with complaints made under an approved privacy code, but the amended subsection will no longer do so.

Item 151 Sections 69 and 70A

Item 151 will repeal sections 69 and 70A.

Section 69 currently prevents the Commissioner from collecting personal information about a third party without that individual's consent. Repealing this section will mean that when handling a privacy complaint, the Commissioner will be allowed to collect personal information about an individual who is not the complainant. This will implement the Government's acceptance of ALRC Recommendation 49-12, and will improve the Commissioner's ability to resolve complaints. This is in line with other similar Commonwealth regulatory bodies that do not have this restriction on their investigation functions. For example, the ALRC noted that there was no equivalent provision in the *Human Rights and Equal Opportunity Act 1986* (Cth) or other State and Territory privacy legislation.

As an APP entity, the OAIC will be subject to the APPs in its handling of that third party personal information.

Item 152 Subsection 72(1)

Item 152 will repeal subsection 72(1).

Subsection 72(1) deals with determinations regarding breaches of an IPP. The IPPs will be repealed by amendments in Schedule 1 and replaced by the APPs. Subsection 72(1) will therefore no longer be necessary. Subsection 72(2) will be amended to deal with breaches of the APPs in item 154 below.

Item 153 Subsection 72(2) (heading)

Item 153 will repeal and replace the heading to subsection 72(2). This will remove the reference to an 'organisation' and replace it with a reference to an 'APP entity', thereby reflecting changes which will be brought about by amendments in Schedule 1.

Item 154 Paragraph 72(2)(a)

Item 154 will repeal and replace paragraph 72(2)(a). This will remove the references to 'organisations', 'approved privacy codes' and the NPPs, which will be replaced by references to 'APP entities', 'registered APP codes' and the APPs respectively. This will reflect changes which will be brought about by amendments in Schedule 1.

Item 155 Paragraph 72(2)(b)

Item 155 will amend paragraph 72(2)(b) by removing the word 'organisation' and replacing it with the word 'entity'. The term 'entity' here refers back to the term 'APP entity' in paragraph 72(2)(a), rather than the broader defined term 'entity'.

This will reflect changes which will be brought about by amendments in Schedule 1 and maintain consistency with an earlier amendment to paragraph 72(2)(a).

Item 156 Paragraph 72(2)(b)

Item 156 will amend paragraph 72(2)(b) by de-capitalising the word 'principle'. This is a minor technical amendment made for consistency with current drafting practice.

Item 157 Subsection 72(2)

Item 157 will amend subsection 72(2) by removing the words 'make a written' and replacing them with the words 'by legislative instrument, make a'.

This amendment is necessary because of changes made by the Legislative Instruments Act. This is not a policy change because it does not change the status of the determination as a legislative instrument. Rather, it amends the provision to reflect the actual status of the determination as a legislative instrument.

Item 158 Subsection 72(3)

Item 158 will amend subsection 72(3) by removing the references to an 'organisation' and replacing them with references to an 'APP entity' and also by removing the reference to section 16A and replacing it with a reference to sections 15 and 26A.

The change from ‘organisation’ to ‘APP entity’ will reflect earlier amendments which repealed subsection 72(1) and amended subsection 72(2) to refer to APP entities rather than organisations. This will reflect changes which will be brought about by amendments in Schedule 1.

Item 159 Subsection 72(4)

Item 159 will amend subsection 72(4) by removing the words ‘make a written’ and replacing them with the words ‘by legislative instrument, make a’.

This amendment is necessary because of changes made by the Legislative Instruments Act. This is not a policy change because it does not change the status of the determination as a legislative instrument. Rather, it amends the provision to reflect the actual status of the determination as a legislative instrument.

Item 160 Subsection 72(4)

Item 160 will amend subsection 72(4) by removing the word ‘organisation’ and replacing it with the term ‘APP entity’ and also by removing the reference to section 16A and replacing it with a reference to sections 15 and 26A.

The change from ‘organisation’ to ‘APP entity’ will give the Commissioner the discretion to provide that any public interest determination may have general effect. Currently, subsections 72(4) and (5) only provide for the Commissioner to give general effect to determinations that apply to organisations. However, the OAIC has advised that circumstances have arisen where it would have been beneficial to provide for a determination in relation to an agency to have general effect. For example, it will allow the Commissioner to make a public interest determination that has general effect in relation to agencies, rather than require the Commissioner to make separate public interest determinations in relation to each agency separately. This will improve administrative efficiency.

Item 161 Subsection 72(4)

Item 161 will amend subsection 72(4) by removing the words ‘organisation does’ and replacing them with the words ‘APP entity does’. This will reflect an earlier amendment expanding the application of this subsection to include public interest determinations in relation to agencies.

Item 162 Subsection 72(4)

Item 162 will amend subsection 72(4) by removing the phrase ‘organisation or any other organisation’ and replacing it with the phrase ‘entity or any other APP entity’. This will reflect an earlier amendment expanding the application of this subsection to include public interest determinations in relation to agencies.

Item 163 Section 73 (heading)

Item 163 will repeal and replace the heading to section 73. This will remove the words ‘agency or organisation’ and replace them with the term ‘APP entity’. This will reflect changes which will be brought about by amendments in Schedule 1 that replace the IPPs and NPPs with the APPs.

Item 164 Subsection 73(1)

Item 164 will amend subsection 73(1) by removing the words 'an agency or organisation' and replacing them with the term 'an APP entity'. This will reflect changes which will be brought about by amendments in Schedule 1 that replace the IPPs and NPPs with the APPs.

Item 165 Subsection 73(1)

Item 165 will amend subsection 73 (1) by removing the words 'the agency or organisation' and replacing them with the words 'the entity'. This will reflect changes which will be brought about by amendments in Schedule 1 that replace the IPPs and NPPs with the APPs.

Item 166 After subsection 73(1)

Item 166 will amend section 73 by inserting a new subsection 73(1A).

This new subsection 73(1A) will give the Commissioner the discretion to dismiss an entity's application for a public interest determination if the Commissioner is satisfied that the application is frivolous, vexatious, misconceived, lacking in substance or not made in good faith. Currently, once a formal application is made, the Commissioner cannot dismiss such an application without considerable consultation and related processes.

This will implement the Government's response to ALRC Recommendation 47-8, in respect of applications which the Commissioner is satisfied are frivolous, vexatious or misconceived. This means an application may be dismissed outright and should act as an encouragement for applicants to discuss applications with the Commissioner before submitting them. The inclusion of applications which the Commissioner is satisfied are lacking in substance or not made in good faith will create consistency with sections 54W and 73 of the FOI Act.

Item 167 Section 74 (heading)

Item 167 will repeal and replace the heading to section 74. This will reflect a later amendment which will expand the content of section 74 to require the Commissioner to publish notice of the dismissal of an application. Adding the word 'etc.' to the end of the heading will indicate that the section will deal with more than just the publication of applications.

Item 168 Subsection 74(1)

Item 168 will amend subsection 74(1) by removing and replacing all of the words after 'notice'. The amended subsection will provide that, in addition to publishing notice of applications received, the Commissioner shall publish notice of the dismissal of any application dismissed by the Commissioner under the new subsection 73(1A). This additional requirement will ensure that there is transparency about the handling of applications for public interest determinations.

Item 169 At the end of subsection 75(1)

Item 169 will amend subsection 75(1) to incorporate a reference to the new subsection 73(1A). The amended subsection will confirm that the Commissioner does not need to prepare a draft of a proposed public interest determination if the Commissioner dismisses the application under the new subsection 73(1A).

Item 170 Subsection 79(3)

Item 170 will repeal subsection 79(3). This will mean that the Commissioner is no longer required to include a statement of reasons in a public interest determination. Because of the effect of section 26 of the Legislative Instruments Act, an Explanatory Statement will need to accompany the registration of a legislative instrument. Section 4 of the Legislative Instruments Act provides that an Explanatory Statement should, amongst other things, 'explain the purpose and operation of the instrument'. Such a statement is likely to sufficiently explain the basis for the decision to remake a public interest determination, or temporary public interest determinations. The requirement in subsection 79(3) is therefore unnecessary.

Item 171 Section 80

Item 171 will repeal section 80. This amendment is necessary because of changes made by the Legislative Instruments Act. This is not a policy change because it does not change the status of the determination as a legislative instrument. Rather, it amends the provision to reflect the actual status of the determination as a legislative instrument.

Item 172 Paragraph 80A(1)(a)

Item 172 will amend paragraph 80A(1)(a) by removing the words 'agency or organisation' and replacing them with the term 'APP entity'. This will reflect changes which will be brought about by amendments in Schedule 1 that replace the IPPs and NPPs with the APPs.

Item 173 Subparagraphs 80A(1)(a)(i) and (ii)

Item 173 will repeal and replace subparagraphs 80A(1)(a)(i) and (ii).

This will remove the references in the current paragraphs to the IPPs and NPPs, which will be repealed by amendments in Schedule 1 and replaced by the APPs. The new paragraphs will be consistent with the Schedule 1 amendments by referring to the APPs, registered APP codes and APP entities.

Item 174 Paragraph 80A(1)(b)

Item 174 will amend paragraph 80A(1)(b) by removing the words 'agency or organisation' and replacing them with the word 'entity'. The term 'entity' here refers back to the term 'APP entity' in paragraph 80A(1)(a), rather than the broader defined term 'entity'.

This will reflect changes which will be brought about by amendments in Schedule 1 and maintain consistency with an earlier amendment to paragraph 80A(1)(a).

Item 175 Paragraph 80A(1)(b)

Item 175 will amend paragraph 80A(1)(b) by de-capitalising the word 'principle'. This is a minor technical amendment made for consistency with current drafting practice.

Item 176 Subsection 80A(2)

Item 176 will amend subsection 80A(2) by removing the phrase 'make a written temporary public interest' and replacing it with the phrase 'by legislative instrument, make a'.

This amendment is necessary because of changes made by the Legislative Instruments Act. This is not a policy change because it does not change the status of the determination as a legislative instrument. Rather, it amends the provision to reflect the actual status of the determination as a legislative instrument.

Item 177 Paragraph 80A(2)(a)

Item 177 will amend paragraph 80A(2)(a) by removing the words 'agency or organisation' and replacing them with the term 'APP entity'. This will reflect changes which will be brought about by amendments in Schedule 1 that replace the IPPs and NPPs with the APPs.

Item 178 Subsection 80A(3)

Item 178 will repeal and replace subsection 80A(3). The new subsection 80A(3) will mean that the Commissioner is no longer required to include a statement of reasons in a temporary public interest determination.

Because of the effect of section 26 of the Legislative Instruments Act, an Explanatory Statement will need to accompany the registration of a legislative instrument. Section 4 of that Act provides that an Explanatory Statement should, amongst other things, 'explain the purpose and operation of the instrument'. Such a statement is likely to sufficiently explain the basis for the decision to remake a public interest determination, or temporary public interest determinations. The requirement in paragraph 80A(3)(b) is therefore unnecessary.

Item 179 Subsections 80B(1) and (2)

Item 179 will repeal subsections 80B(1) and (2) and replace them with a new subsection 80B(1).

This will remove the references to 'agencies' and 'organisations', which will be replaced by references to 'APP entities'. This will reflect changes which will be brought about by amendments in Schedule 1 that replace the IPPs and NPPs with the APPs. It will also remove the reference to section 16A and replace it with a reference to sections 15 and 26A. Those provisions provide that APP entities must comply with the APPs or a registered APP code.

Item 180 Subsection 80B(3)

Item 180 will amend subsection 80B(3) by removing the words 'make a written' and replacing them with the words 'by legislative instrument, make a'.

This amendment is necessary because of changes made by the Legislative Instruments Act. This is not a policy change because it does not change the status of the determination as a legislative instrument. Rather, it amends the provision to reflect the actual status of the determination as a legislative instrument.

Item 181 Subsection 80B(3)

Item 181 will amend subsection 80B(3) by removing the reference to an 'organisation' and replacing it with a reference to an 'APP entity' and also by removing the reference to section 16A and replacing it with a reference to sections 15 and 26A. Those provisions provide that APP entities must comply with the APPs or a registered APP code.

The change from ‘organisation’ to ‘APP entity’ will give the Commissioner the discretion to provide that any temporary public interest determination may have general effect. Currently, subsection 80(3) only provides for the Commissioner to give general effect to determinations that apply to organisations. This amendment will mean that the distinction is no longer maintained. This will maintain consistency with an earlier amendment relating to public interest determinations.

Item 182 Subsection 80B(3)

Item 182 will amend subsection 80B(3) by removing the words ‘organisation does’ and replacing them with the words ‘APP entity does’. This will reflect an earlier amendment expanding the application of this subsection to include temporary public interest determinations in relation to agencies.

Item 183 Subsection 80B(3)

Item 183 will amend subsection 80B(3) by removing the words ‘organisation or another organisation’ and replacing them with the words ‘entity or another APP entity’. This will reflect an earlier amendment expanding the application of this subsection to include temporary public interest determinations in relation to agencies.

Item 184 Section 80C

Item 184 will repeal section 80C. This amendment is necessary because of changes made by the Legislative Instruments Act. This is not a policy change because it does not change the status of the determination as a legislative instrument. Rather, it amends the provision to reflect the actual status of the determination as a legislative instrument.

Item 185 Paragraph 80D(2)(a)

Item 185 will amend paragraph 80D(2)(a) by removing the reference to subsections 72(1) and (2) and replacing it with a reference to subsection 72(2) only. This will reflect an earlier amendment which repealed subsection 72(1).

Item 186 Paragraph 80P(1)(a)

Item 186 will amend paragraph 80P(1)(a) by removing the word ‘concerned’. This is a minor technical amendment made for consistency with current drafting practice.

Item 187 Subsections 80P(4) and (5)

Item 187 will repeal subsections 80P(4) and (5) and replace them with a new subsection 80P(4). This will remove the references in the current subsections to agencies, organisations and the IPPs and NPPs, which will be repealed by amendments in Schedule 1 and replaced by the APPs. The new subsection will be consistent with the Schedule 1 amendments by referring to the APPs, registered APP codes and APP entities.

Item 188 Paragraphs 80Q(2)(a) and (b)

Item 188 will repeal paragraphs 80Q(2)(a) and (b) and replace them with a new paragraph 80Q(2)(a).

This will remove the references in the current paragraphs to agencies, organisations and the IPPs and NPPs, which will be repealed by amendments in Schedule 1 and replaced by the APPs. The new paragraph will be consistent with the Schedule 1 amendments by referring to APP entities, the APPs and registered APP codes.

Item 189 After Part VIA

Item 189 will insert a new Part VIB following Part VIA.

Part VIB will deal with civil penalty orders and will consist of three divisions.

Division 1 – Civil penalty provisions

Section 80U will define the phrase 'civil penalty provision' as a section or subsection of the Privacy Act which has at its foot, the words 'civil penalty' and one or more amounts in civil penalty units. This is a standard drafting approach for civil penalty provisions. It is intended to help identify the specific section of sub-section that is contravened in a civil penalty provision. This is important in achieving certainty in potential legal proceedings.

Section 80V will list actions which, if taken by an entity, will constitute ancillary contraventions of civil penalty provisions. This is another standard civil penalty provision. This section provides that there will be a contravention of the provision where anyone:

- attempts to contravene a civil penalty provision
- aids, abets, counsels, procures or induces a contravention
- is knowingly concerned in a contravention of a civil penalty, or
- conspires with others to cause a contravention.

Division 2 – Obtaining a civil penalty order

Division 2 of Part VIB contains a number of machinery provisions relating to the obtaining of a civil penalty order. Subsection 80W(1) allow the Commissioner to apply to the Federal Court or Federal Magistrates Court for a civil penalty order where an entity has contravened a civil penalty provision. The application must be made within 6 years of the alleged contravention.

Under subsection 80W(3), if the court is satisfied that the entity has contravened the civil penalty provision, it may order an entity to pay to the Commonwealth such pecuniary penalty for the contravention as the court determines appropriate. Subsection 80W(5) provides that the maximum penalty the Court can order will be the amount of the pecuniary penalty specified for the provision, unless the entity is a body corporate, in which case the maximum penalty will be an amount five times of that specified for the provision. An example of this is new section 13G (Serious and repeated interferences with privacy) which contains a penalty of 2,000 penalty units. For a body corporate, that penalty with be 10,000 penalty units.

Subsection 80W(6) will provide a non-exhaustive list of matters that the court must take into account in determining the pecuniary penalty, including: the nature and extent of the contravention and any loss or damage suffered because of the contravention; the

circumstances in which the contravention took place, and whether the entity has previously been found by a court to have engaged in any similar conduct.

Section 80X provides that a pecuniary penalty is a debt payable to the Commonwealth, and that it is taken to be a judgement debt, enforceable as if the order were made in civil proceedings against the entity to recover a debt.

Subsection 80Y(1) will provide that proceedings may be instituted under this new Division in relation to the contravention of any one or more civil penalty provisions, if conduct constitutes a contravention of two or more civil penalty provisions. However, subsection 80Y(2) will provide that an entity will not be liable to more than one pecuniary penalty under that Division in relation to the same conduct.

Subsection 80Z(1) will provide that if proceedings for multiple contraventions are founded on the same facts, or the contraventions form, or are part of, a series of contraventions of the same or similar character, then the Court may make a single civil penalty order against the entity. However, subsection 80Z(2) will ensure that the penalty imposed must not exceed the sum of the maximum penalties which could be ordered if imposed for each contravention separately.

Section 80ZA will provide that the Court may direct that two or more proceedings for civil penalty orders be heard together. Section 80ZB will provide that the normal rules of evidence and procedure for civil matters apply to proceedings for a civil penalty order.

Section 80ZC will make it clear that a contravention of a civil penalty order is not an offence.

Division 3 – Civil proceedings and criminal proceedings

Section 80ZD will provide that the Court must not make a civil penalty order against an entity if the entity has been convicted of an offence constituted by the same, or substantially the same, conduct as that constituting the contravention of a civil penalty provision. This is an important safeguard which ensures that an entity is not punished more than once for the same conduct.

Subsection 80ZE(1) will provide that civil penalty proceedings against an entity will be stayed if criminal proceedings are or have already been commenced against the entity for an offence which is constituted by conduct that is the same, or substantially the same, as the conduct alleged to constitute a contravention of a civil penalty provision. Subsection 172(2) will provide that unless the entity is not convicted of the offence, the proceedings are dismissed and costs must not be awarded. However if the entity is not convicted of the offence, the civil penalty proceedings may be resumed. This is an important safeguard which ensures that an entity is not subjected to civil proceedings for the same conduct that is being dealt with under criminal proceedings.

Section 80ZF will provide that regardless of whether a civil penalty order has been made against an entity, criminal proceedings may be commenced against the entity for conduct that is that same, or substantially the same, as conduct that would constitute a contravention of a civil penalty provision. This provision makes it clear that an entity could be subjected to criminal proceedings for the same conduct that has attracted a civil penalty order. This makes it clear that criminal proceedings take precedence and cannot be avoided by a prior civil penalty order.

Section 80ZG will provide that particular evidence given by an individual in proceedings against them for a civil penalty order is not admissible in criminal proceedings against the individual if the conduct alleged to constitute the offence is the same, or substantially the same, as the conduct alleged to constitute the contravention of a civil penalty provision. Subsection 174(2) will provide that the general rule of inadmissibility will not apply in criminal proceedings relating to the falsity of evidence given in the civil penalty proceedings.

Item 190 After paragraph 82(2)(a)

Item 190 will amend subsection 82(2) by inserting a new paragraph 82(2)(aa).

This new subsection will make the Privacy Commissioner a member of the Privacy Advisory Committee.

Item 191 Paragraph 82(2)(b)

Item 191 will amend paragraph 82(2)(b) by removing the words '6 other' and replacing them with the words '8 other'. This will increase the membership of the Privacy Advisory Committee from 6 members other than the Commissioner to 8 members other than the Commissioner and the Privacy Commissioner. This will enable the Government to appoint a more diverse cross-section of the community to the Privacy Advisory Committee.

Item 192 Subsection 82(3)

Item 192 will amend subsection 82(3) by inserting a reference to the Privacy Commissioner following the reference to the Commissioner. This will reflect an earlier amendment which made the Privacy Commissioner a member of the Privacy Advisory Committee'.

Item 193 Paragraph 82(7)(a)

Item 193 will repeal paragraph 82(7)(a) and replace it with three new paragraphs 82(7)(a),(aa) and (ab).

This will create separate requirements for appointed members with at least 5 years' experience in industry or commerce (paragraph 82(7)(a)) and experience in public administration or the service of a government or an authority of a government (paragraph 82(7)(aa)). These areas of experience are currently a combined requirement of paragraph 82(7)(a). This will ensure that the Government has the discretion to appoint such members separately in order to fairly represent private and public sector interests.

It will also create a requirement for a member with extensive experience in health privacy (paragraph 82(7)(ab)). This will implement the Government's response to ALRC Recommendation 46-4(b).

Item 194 Paragraph 82(7)(b)

Item 194 will amend paragraph 82(7)(b) by removing the word 'shall' and replacing it with the word 'must'. This is a minor technical amendment made for consistency with current drafting practice.

Item 195 At the end of paragraph 82(7)(b)

Item 195 will amend paragraph 82(7)(b) by inserting the word 'and' at the end of the paragraph. This is a minor technical amendment made for consistency with current drafting practice.

Item 196 Paragraph 82(7)(c)

Item 196 will repeal and replace paragraph 82(7)(c).

The new paragraph will create a requirement for a member with experience in information and communication technologies, and will replace the requirement for experience in electronic data-processing. This will implement the Government's response to ALRC Recommendation 46-4(c) by updating the language of the criterion. The ALRC's view was that this terminology should be included to 'reflect more contemporary practices and parlance'.

Item 197 Paragraphs 82(7)(d) and (e)

Item 197 will amend paragraphs 82(7)(d) and (e) by removing the word 'shall' and replacing it with the word 'must'. This is a minor technical amendment made for consistency with current drafting practice.

Item 198 Paragraph 83(b)

Item 198 will amend paragraph 83(b) by removing the reference to 'guidelines' and replacing it with a reference to 'rules or guidelines'.

This will reflect the change in terminology throughout the Privacy Act implementing the Government's acceptance of ALRC Recommendation 47-2. The word 'rules' will be used where appropriate to more accurately reflect the binding nature of certain guidelines and to distinguish binding instruments issued or approved by the Privacy Commissioner from voluntary guidance.

Amendments have not been made to change the binding guidelines made under sections 95, 95A and 95AA to 'rules'. This is because other Acts also refer to those guidelines and making changes would create inconsistencies in those other Acts.

It will therefore be necessary for paragraph 83(b) to refer to both rules and guidelines.

Item 199 Subsections 95(5), 95A(7) and 95AA(3)

Item 199 will repeal subsections 95(5), 95A(7) and 95AA(3).

These subsections each provide that an application may be made to the Administrative Appeals Tribunal (AAT) for review of certain decisions of the Commissioner. The contents of each of the subsections will be reproduced in the new section 96, which will be introduced to deal specifically with appeals to the AAT. The existing subsections will therefore no longer be necessary.

Item 200 After section 95C

Item 200 will insert a new section 96 following section 95C.

This new section 96 will implement ALRC Recommendation 49-7 by expanding the availability of merits review by the AAT of determinations made by the Commissioner. The former section 61, which will be repealed, only provided for review by the AAT in limited circumstances. The new section 96 will allow for review of all decisions by the Commissioner under subsections 52(1) and (1A) to make a determination. It will also apply to: decisions not to register certain APP codes and CR codes; decisions dismissing frivolous, vexatious etc. applications for a public interest determination; and decisions not to approve certain medical research guidelines. Increasing the availability of merits review is intended to promote further transparency and accountability in the Commissioner's decisions.

Item 201 After section 98

Item 201 will insert new sections 98A, 98B and 98C following section 98. These will deal with the treatment of partnerships, unincorporated associations and trusts respectively. These are based on standard existing provisions that are used in a number of other Commonwealth Acts which outline when vicarious liability might apply to these types of entities. These provisions recognise that, in appropriate circumstances, particular individuals within partnerships, unincorporated associations and trusts, should be responsible for civil contraventions and criminal offences committed by those entities. It is important to ensure that any civil contraventions and criminal offences committed by these types of entities (which are not legal persons) can be proceeded with through the courts.

A safeguard in each case is that an offence will not be committed, or a civil penalty provision contravened, if the partner, or member of an unincorporated association's committee of management, or trustee:

- does not know of the circumstances that constitute the contravention of the provision concerned, or
- knows of those circumstances but takes all reasonable steps to correct the contravention as soon as possible after the trustee, partner, or the member of an unincorporated association's committee, becomes aware of those circumstances.

In criminal proceedings, a defendant will bear an evidential burden for these matters in accordance with subsection 13.3(3) of the Criminal Code.

Item 202 Subsection 99A(1)

Item 202 will amend subsection 99A(1) by inserting the words 'or for a civil penalty order' following the words 'this Act'.

This will extend the reach of the subsection, which is concerned with establishing the state of mind of a body corporate for liability purposes, to apply to proceedings for a civil penalty order in addition to proceedings for an offence against the Privacy Act. This is required because of the introduction of the civil penalty provision regime.

Item 203 Subsection 99A(2)

Item 203 will amend subsection 99A(2) by inserting the words ‘or proceedings for a civil penalty order’ following the words ‘this Act’.

This will extend the reach of the subsection to deem certain conduct to be conduct engaged in by a body corporate for the purposes of proceedings for a civil penalty order in addition to prosecution for an offence against the Privacy Act. This is required because of the introduction of the civil penalty provision regime into the Privacy Act.

Item 204 Subsection 99A(3)

Item 204 will amend subsection 99A(3) by inserting the words ‘or for a civil penalty order’ following the words ‘this Act’.

This will extend the reach of the subsection, which is concerned with establishing the state of mind of a person other than a body corporate for liability purposes, to apply to proceedings for a civil penalty order in addition to proceedings for an offence against the Privacy Act. This is required because of the introduction of the civil penalty provision regime into the Privacy Act.

Item 205 Subsection 99A(4)

Item 205 will amend subsection 99A(4) by inserting the words ‘or proceedings for a civil penalty order’ following the words ‘this Act’.

This will extend the reach of the subsection to deem certain conduct to be engaged in on behalf of a person other than a body corporate for the purposes of proceedings for a civil penalty order in addition to prosecution for an offence against the Privacy Act. This takes account of the introduction of the civil penalty provisions into the Privacy Act.

Item 206 Subsection 99A(9)

Item 206 will repeal subsection 99A(9).

This subsection will no longer be necessary, because of an earlier amendment which inserted a definition of ‘offence against this Act’ into subsection 6(1). The new definition includes the same sections of the *Crimes Act 1914* and *Criminal Code* as are included in the repealed subsection 99A(9).

Schedule 5—Amendments of other Acts

This schedule makes amendments to other Acts that are consequential to the amendments to the Privacy Act in Schedules 1 to 4.

Part 1—Amendments relating to the Australian Privacy Principles

Definition of Australian Privacy Principle

Item 1 inserts a definition of 'Australian Privacy Principle' into section 2B of the Acts Interpretation Act. This ensures that when the term 'Australian Privacy Principle' is used in another Act it is not necessary to include a definition of the term.

Referring to APPs instead of IPPs or NPPs

Several items replace references to the IPPs or NPPs with corresponding references to the APPs in various Acts.

The following items make this amendment: 2–4, 6, 9, 10, 13–17, 19–21, 23, 25, 26, 28, 29, 33, 35, 42, 44, 46–52, 54–56, 58, 59, 61, 62, 64, 65, 67, 69, 74, 76–79, 81–93, 96–99 and 101.

Definition of personal information

Several items amend an Act by replacing its definition of 'personal information' with the amended definition in subsection 6(1) of the Privacy Act. This amendment ensures definitional consistency across Acts.

The following items make this amendment: 5, 36, 43, 45, 60, and 73.

Referring to law

Several items amend an Act by replacing relevant references to 'law' with 'this Act'. For example, paragraph 219GA(7) of the *A New Tax System (Family Assistance)(Administration) Act 1999*, as amended by this Schedule, provides that, 'For the purposes of (a) disclosures under paragraph 6.2(b) of APP 6 and (b) a provision of a law of a State or Territory that provides that information that is personal may be disclosed if the disclosure is authorised by law; the disclosure of personal information by a person in response to a notice given under this section is taken to be a disclosure 'that is authorised by law.' The paragraph is amended to refer to disclosure 'that is authorised by this Act'. This is ensures that such disclosures will continue to be authorised disclosures under the Privacy Act.

The following items make similar amendments: 7–9, 11, 12, 14, 15, 18, 21, 22, 24, 28, 30–32, 34, 35, 53, 55–58, 62, 63, 66, 68, 70, 72, 75, 80, 94, 95, 98 and 101.

Healthcare Identifiers Act

Item 37 repeals the definition of 'National Privacy Principle' as it is no longer relevant.

Item 38 repeals subsection 9(6), which referred to NPP 7, and replaces it with a new subsection 9(6) providing that a healthcare identifier is a government related identifier for the purposes of the Privacy Act. APP 9 deals with the adoption, use or disclosure of government related identifiers. 'Identifier' is defined in subsection 6(1) of the Privacy Act, see item 25 of Schedule 1.

Items 39 and 40 amend section 18 and paragraph 23(b) respectively by replacing references to NPP 2 with a broader reference to the Act as 'responsible person' is now defined in new section 6AA of the Privacy Act. See item 52 of Schedule 1.

Item 41 amends paragraph 26(2)(c) by referring to new section 16 of the Privacy Act (personal, family or household affairs) instead of section 16E, which referred to the NPPs.

Record keeper

Items 27 and 100 replace references to a 'record keeper who has possession or control of' with references to 'An APP entity that holds' as the concept of 'record keeper' is no longer relevant to the new APPs. See items 73 – 75 of Schedule 1 which amend section 10 of the Privacy Act. New section 10 provides for when an agency is taken to hold a record.

Other amendments

Item 71 amends paragraph 73(b) of the Personally Controlled Electronic Health Records Act to remove a reference to section 13A of the Privacy Act as this section is repealed by item 42 of Schedule 4.

Part 2—Amendments relating to credit reporting

Referring to credit reporting bodies instead of credit reporting agencies

Several items amend an Act by replacing references to 'credit reporting agencies' with references to 'credit reporting bodies'. This reflects the new credit reporting regime which applies to 'credit reporting bodies' rather than 'credit report agencies'. See items 25 and 26 of Schedule 2.

The following items make this amendment: 102, 104–114, 116–118, 120, 121, 123–126, 128 and 129–133.

References to credit information files

Several items amend an Act by removing references to a 'credit information file'.

The term 'credit information file' will not appear in the amended Privacy Act as it has become obsolete. A credit information file was a record kept by a credit reporting agency that contained information relating to an individual kept in the course of carrying on a credit reporting business. Due to advances in technology and changes to the way data flows through and is held in the credit reporting system, the idea of a credit information file is no longer accurate. Information is no longer held in a file, per se, but sits in various systems and can be brought together into a package about a particular individual at a particular time. See item 22 of Schedule 2 which repeals the definition of 'credit information file'.

The following items make this amendment: 103, 109, 112, 115, 118–121 and 134.

Other amendments

Item 122 amends subsection 35B(3) of the Anti-Money Laundering and Counter-Terrorism Financing Act by replacing a reference to paragraph 18K(1)(m) of the Privacy Act with a reference to paragraph 20E(3)(e) of the amended Privacy Act. The paragraphs have the same effect, namely to make an exception to the rule against disclosure of personal information when the disclosure is required or authorised by law.

Item 127 amends section 35L of the Anti-Money Laundering and Counter-Terrorism Financing Act by removing the reference to section 13A of the Privacy Act as this section is repealed by item 42 of Schedule 4.

Part 3—Amendments relating to codes

Item 135 amends the Australian Information Commissioner Act by amending the wording of paragraph 32(1)(b) to reflect the introduction of APP codes by Schedule 3.

Items 136–146 amend the Telecommunications Act and the *Telecommunications (Consumer Protections and Service Standards) Act 1999* by replacing the words 'an approved privacy code' with 'a registered APP code'. The amendments reflect the introduction of APP codes by Schedule 3.

Part 4—Other amendments

Functions and powers of the Commissioner

Several items amend Acts to reflect the consolidation of the powers and functions of the Commissioner by item 54 of Schedule 4.

Item 147 amends paragraph 20(4A)(b) of the *Australian Human Rights Commission Act 1986* by referring to new section 13 of the Privacy Act rather than paragraphs 27(1)(a) or 28(1)(b) or (c) which are no longer appropriate following the amendments made by item 54 of Schedule 4. New section 12 deals with interferences of privacy, see item 42 of Schedule 4.

Several items amend the Australian Information Commissioner Act to either repeal or amend references to sections 27-29 of the Privacy Act to reflect the changes made by item 54 of Schedule 4. The following items make this amendment: 149, 150, 152, 153 and 155.

Correction of errors

Item 148 amends subsection 9(2) of the Australian Information Commissioner Act by omitting a reference to the Schedule to the Data-matching Program (Assistance and Tax) Act, which has been repealed.

Item 156 amends subsection 85ZZG(1) of the Crimes Act by omitting a reference to section 96 of the Privacy Act which has been repealed.

Item 162 amends subsection 13(7) of the Data-matching Program (Assistance and Tax) Act by referring to Part V of the Privacy Act and deleting a reference to section 99 of the Privacy Act which has been repealed.

Referring to rules instead of guidelines

This change in terminology will implement ALRC Recommendation 47-2. The word 'rules' will be used where appropriate throughout the Act to more accurately reflect the binding nature of certain guidelines and to distinguish binding instruments issued by the Privacy Commissioner from voluntary guidance.

The following items make this amendment to various Acts: 151, 154, 157–161, 163 and 165–180.

Other amendments

Item 164 amends subsection 29(3) of the Healthcare Identifiers Act by referring to paragraph 33C(1)(a) of the amended Privacy Act instead of the repealed paragraph 27(1)(h), which had the same effect. See item 64 of Schedule 4.

Schedule 6—Application, transitional and savings provisions

Part 1—Definitions

Item 1 Definitions

Item 1 defines the terms ‘commencement time’, ‘Privacy Act’ and ‘transition period’ as they are used in Schedule 6. The ‘commencement time’ is the day Schedule 1 commences. The table at clause 2 of the Bill states that Schedule 1 commences nine months after Royal Assent. The ‘transition period’ is the time between Royal Assent and ends immediately before the commencement time.

Part 2—Provisions relating to Schedule 1 to this Act

Item 2 Application—court/tribunal orders

Item 2 provides that the definition of ‘court/tribunal order’ inserted by Schedule 1 applies in relation to an order, direction or other instrument made before or after the commencement time. This means that an order, direction or other instrument made before the commencement time by a court or tribunal satisfies the definition of a court/tribunal order for the purposes of all of the new provisions in the Act (including those provisions inserted by the other Schedules).

Item 3 Saving—guidelines relating to medical research etc.

Item 3 has the effect that guidelines made under the Act relating to medical research, health information and genetic information made before the commencement time will continue after the commencement time.

Part 3—Provisions relating to Schedule 2 to this Act

Item 4 Application—credit reporting

Subclause (1) of item 4 provides that the credit reporting provisions in the amended Act apply in relation to credit applied for, or provided, before or after the commencement time. This means that ‘consumer credit liability information’ (which includes four of the new types of personal information introduced by more comprehensive credit reporting in the new Part IIIA) may be disclosed by credit providers to credit reporting bodies in relation to existing credit accounts open at the commencement time, and not just in relation to new accounts opened after the commencement time.

Subclauses (2) and (3) provide that the definitions of ‘court proceedings information’ (subclause 2) and ‘serious credit infringement’ (subclause 3) inserted into the Act by Schedule 2 of the Bill (see items 12 and 63 respectively) apply in relation to a judgement of an Australian court or, for serious credit infringements, an act done, that occurred before the commencement time as well as to a judgement or act done after the commencement time.

Subclause (4) provides that publicly available personal information about the individual that relates to the individual’s activities in Australia or the external Territories and the individual’s credit worthiness, and which is not court proceedings information or information

about the individual that is recorded on the National Personal Insolvency Index, is credit information within the meaning of Clause 6N in Schedule 2, whether the activities to which the publicly available personal information relate were done before or after the commencement time.

Subclause (5) provides that the definition of 'information request' in clause 6R, in Schedule 2, will apply to an information request made before or after the commencement time.

Subclause (6) sets the commencement time for the provisions relating to repayment history information in clause 6V, inserted by Schedule 2 of the Bill. The definition of 'repayment history information' includes whether or not the individual has met an obligation to make a monthly payment that is due and payable in relation to the consumer credit, the day on which the monthly payment is due and payable, and, if the individual makes the monthly payment after the day on which the payment is due and payable, then the day on which the individual makes the payment. In addition, clause 6V states that the regulations may make provision in relation to certain matters, including whether or not a payment is a monthly payment. Subclause (6) provides that the definition of repayment history in clause 6V will only apply to a monthly payment that is due and payable on or after the day of Royal Assent. This means that credit providers can disclose 9 months of repayment history information to credit reporting bodies at the commencement of the new provisions. However, any obligations or other requirements in relation to repayment history information, whether contained in the credit reporting provisions or set out in regulations or the registered CR Code, must be satisfied before the repayment history information can be disclosed to, and collected by, any credit reporting body after commencement of the credit reporting provisions.

Part 4—Provisions relating to Schedule 3 to this Act

Item 5 Privacy codes may be developed etc. during the transition period

Subclause (1) provides that any function or power conferred on the Commissioner or an entity by Part IIIB, inserted by Schedule 3, may be performed or exercised during the transition period as if the amended Privacy Act was in force during that period. The effect of this provision is that APP codes and the CR Code may be developed and registered during the transition period. Subclause (2) provides that the performance of any function or the exercise of any power during the transition period has effect after the commencement time as if that function had been performed or that power had been exercised under Part IIIB. The effect of this provision is that actions taken in relation to any APP code or the CR Code during the transition period will be taken, after the commencement time, to have been done under Part IIIB. This means that the CR Code can be developed and, if the Commissioner is satisfied of the matters required in Part IIIB, registered during the transition period and that registered CR Code will be effective immediately after the commencement time. The registered CR Code is an essential requirement for the practical operation of the credit reporting provisions. These transitional arrangements provide a mechanism for the CR Code to be developed and registered during the transition period.

Part 5—Provisions relating to Schedule 4 to this Act

Item 6 Application—section 13G of the Privacy Act

Item 6 provides that the new section 13G of the Privacy Act—a civil penalty provision concerning serious and repeated interferences with privacy—applies only in relation to acts or practices which occurred after the commencement time. The item avoids the possibility of retrospective punishment.

Item 7 Saving—guidelines relating to tax file number information

Item 7 provides that guidelines relating to tax file number information made under subsection 17(1) of the Privacy Act that were in force immediately before the commencement time will remain in effect after the commencement time.

Item 8 Saving—guidelines prepared and published under the Privacy Act

Item 8 provides that guidelines prepared and published under paragraphs 27(1)(e) or 28A(1)(e) relating to interferences with individual privacy will continue to apply after the commencement time.

Item 9 Audits by the Commissioner

Item 9 provides that if the Commissioner commenced an audit under paragraphs 27(1)(h) or (ha) or 28(1)(e) or 28A(1)(g) of the Privacy Act before the commencement time, the Commissioner may continue the audit after the commencement time as if the amendments had not been made.

Item 10 Application—amendment made by item 75 of Schedule 4

Item 10 provides that the amendment to subsection 38B(2) of the Privacy Act, which allows class members to withdraw from representative complaints if the complaint was made without their consent, applies to representative complaints made after the commencement time.

Item 11 Application—paragraph 41(1)(db) of the Privacy Act

Paragraph 41(1)(db) provides that the Commissioner may decide not to investigate, or stop investigating, a complaint if the complainant has not responded to a request by the Commissioner for information within a specified period. Item 11 provides that this paragraph applies to requests made after the commencement time.

Item 12 Saving—public interest determinations

Item 12 provides that determinations made under section 72 of the Privacy Act before the commencement time will remain in effect after the commencement time. Further, Item 12 provides a process for the Commissioner to vary such determinations after the commencement time to take into account amendments to the Privacy Act.

Item 13 Application—subsection 73(1A) of the Privacy Act

Item 13 provides that the new section 73(1A) of the Privacy Act applies to applications for a public interest declaration made under section 73(1) after the commencement time.

Section 73 provides that an agency or organisation may apply in accordance with the regulations for a determination under section 72 about an act or practice of the agency or organisation (see items 56–63 of Schedule 4).

The new section 73(1A) of the Privacy Act provides that the Commissioner may, in writing, dismiss an application made under section 73(1) if he or she is satisfied that the application is frivolous, vexatious, misconceived, lacking in substance or not made in good faith (see item 67 of Schedule 4).

Item 14 Application—review by the Administrative Appeals Tribunal

Item 14 provides that paragraphs 96(1)(c), (e), (f) and (g) as inserted into the Privacy Act by item 76N of Schedule 4 apply in relation to decisions made after the commencement time.

Paragraph 96(1)(c) provides that the AAT may review decisions by the Commissioner under subsections 52(1) or 52(1A) of the Privacy Act in relation to complaints made under the Privacy Act.

Paragraphs 96(1)(e), (f) and (g) provide that the AAT may review decisions by the Commissioner under section 95, subsection 95A(2), subsection 95A(4), subsection 95AA(2) or subsection 95A(6) to refuse approval to or revoke guidelines made under the Privacy Act.

Part 6—Provisions relating to Schedule 5 to this Act

Item 15 Saving—guidelines issued under other Acts

Item 15 provides that guidelines issued under section 135AA of the National Health Act or section 12 of the Data-matching Program (Assistance and Tax) Act before the commencement time will continue to have effect after the commencement time as if they had been rules issued under those sections as amended by Schedule 5 of this Bill.

Part 7—Provisions relating to other matters

Item 16 Pre-commencement complaints

Item 16 relates to complaints about interferences with individual privacy made under section 36 of the Privacy Act before the commencement time. It provides that such complaints will continue to be dealt with after the commencement time as if the amendments to the Privacy Act had not been made unless: (a) the Commissioner has decided under Part V of the Privacy Act not to investigate or further investigate the subject of the complaint; or (b) has made a determination in relation to the complaint under section 52.

Item 17 Pre-commencement own initiative investigations

Item 17 provides that, after the commencement time, the Commissioner may continue any incomplete investigations begun under subsection 40(2) before the commencement time as if the amendments to the Privacy Act had not been made.

Item 18 Pre-commencement acts and practices

Item 18 relates to acts or practices occurring before the commencement time which may have been interferences with individual privacy under the Privacy Act as it was before the commencement time. It provides that, after the commencement time, individuals may make complaints to the Commissioner about acts or practices which may have been interferences with privacy under sections 13 or 13A of the Privacy Act—and which occurred before the commencement time—as if the amendments to the Privacy Act had not been made. Item 18 also provides that the Commissioner may investigate the subject of the complaint as if the Privacy Act had not been amended.

Item 19 Regulations may deal with transitional etc. matters

Item 19 provides that the Governor-General may make regulations dealing with matters of a transitional, application or saving nature relating to amendments made to the Privacy Act.