# Explanatory Statement

*Privacy (International Money Transfers) Temporary Public Interest Determination 2014 (No. 1)* and *Privacy (International Money Transfers) Generalising Determination 2014 (No. 1)*

This explanatory statement has been prepared by the Privacy Commissioner, in accordance with the functions and powers conferred on him by section 12 of *the Australian Information Commissioner Act 2010* (the Australian Information Commissioner Act).

It explains the purpose and intended operation of the *Privacy (International Money Transfers) Temporary Public Interest Determination 2014 (No. 1)* (TPID 2014-1) made under subsection 80A(2) of the *Privacy Act 1988* (Privacy Act) and *Privacy (International Money Transfers) Generalising Determination 2014 (No. 1)*  (GD 2014-1) made under subsection 80B(3) of the Privacy Act.

## Authority for the Rule

The Australian Information Commissioner is empowered by subsection 80A(2) of the Privacy Act to make TPID 2014-1.

Subsection 80A(2) of the Privacy Act states:

The Commissioner may, by legislative instrument, make a determination that he or she is satisfied of the matters set out in subsection (1). The Commissioner may do so:

1. on request by the APP entity
2. on the Commissioner’s own initiative.

Subsection 80A(1) states:

This section applies if the Commissioner is satisfied that:

1. the act or practice of an APP entity that is the subject of an application under section 73 for a determination under section 72 breaches, or may breach:
2. an Australian Privacy Principle; or
3. a registered APP code that binds the entity; and
4. the public interest in the entity doing the act, or engaging in the practice, outweighs to a substantial degree the public interest in adhering to that principle or code; and
5. the application raises issues that require an urgent decision.

The Australian Information Commissioner is empowered by subsection 80B(3) of the Privacy Act to make GD 2014-1.

Subsection 80B(3) states:

The Commissioner may, by legislative instrument, make a determination that no APP entity is taken to contravene section 15 or 26A if, while that determination is in force, an APP entity does an act, or engages in a practice, that is the subject of a temporary public interest determination in relation to that entity or another APP entity.

Subsection 6(1) of the Privacy Act defines ‘Commissioner’ to mean ‘the Information Commissioner within the meaning of the *Australian Information Commissioner Act 2010*.’

As a ‘privacy function’, TPID 2014-1 and GD 2014-1 can be made by the Privacy Commissioner in accordance with the functions and powers conferred on the Privacy Commissioner by section 12 of the Australian Information Commissioner Act.

## Purpose

The purpose of TPID 2014-1 and GD 2014-1 is to permit Australia and New Zealand Banking Group Limited (Applicant) and other authorised-deposit taking institutions within the meaning of the *Banking Act 1959* (ADIs) to disclose the personal information of a beneficiary of an international money transfer (IMT) to an overseas financial institution when processing an IMT without breaching the Australian Privacy Principles (APPs), following the commencement of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Privacy Amendment Act). Specifically, TPID 2014-1 and GD 2014-1 will ensure that the Applicant and other ADIs do not breach APP 8.1 when disclosing the beneficiary’s personal information to the overseas financial institution, and are not held to breach another APP (other than APP 1) as a result of being held accountable for an act or practice of the overseas financial institution in relation to that information (in accordance with subsection 16C(2)).

In making TPID 2014-1 and GD 2014-1, the Privacy Commissioner has had regard to the objects of the Privacy Act, in particular:

* to promote the protection of the privacy of individuals (paragraph 2A(a))
* to recognise that the protection of the privacy of individuals is balanced with the interest of entities in carrying out their functions and activities (paragraph 2A(b))
* to promote responsible and transparent handling of personal information by entities (paragraph 2A(d)), and
* to facilitate the free flow of information across national borders while ensuring that the privacy of individuals is respected (paragraph 2A(f)).

## Application for a Public Interest Determination

On 24 February 2014, the Applicant made an application under subsection 73(1) of the Privacy Act for a public interest determination under subsection 72(2) of the Privacy Act, and a temporary public interest determination under subsection 80A(2) of the Privacy Act (Application). The Application suggested that if either determination is made, generalising determinations should be made under subsection 72(4) and subsection 80B(3) of the Privacy Act respectively to apply to all ADIs.

The Application indicated a concern that, in the absence of the determinations, the Applicant and other ADIs may breach APP 8.1 when processing an IMT, and may be taken to breach another APP (other than APP 1) as a result of being held accountable for an act or practice of an overseas financial institution, in circumstances where it is not practicable for the Applicant to take further steps to prevent such breaches.

The Application provided an outline of the IMT process:

* An international money transfer (IMT) is the term used for a payment made by an Australian sender to a beneficiary outside Australia. An IMT requires an ADI to disclose to an overseas financial institution the personal information of the individual that is the beneficiary of the IMT. That personal information will generally include the name and account information of the beneficiary. However, some overseas financial institutions require further information to be provided, such as account name and residential address of the beneficiary, generally because of in-country regulatory requirements, anti-money laundering and counter-terrorism financing (AML/CTF) requirements or to allow sanction checks to be performed onshore.
* Once the sender has completed the request, the Applicant will send the IMT to the beneficiary’s financial institution for payment.
* In the majority of cases, IMTs in Australia are processed using the ‘SWIFT’ network, a secure and highly confidential network which facilitates the transfer of payments and other financial messages between SWIFT users. Once a financial institution becomes a SWIFT user, it establishes ‘account relationships’ (either by contract or through a SWIFT Relationship Management Application) with other users that allow for the processing of IMTs.
* If an ADI does not have an ‘account relationship’ with the beneficiary’s overseas financial institution, it may still transfer money using SWIFT by sending payment instructions to an ‘intermediary bank’ (also a SWIFT user) which will then route the payment instructions to the beneficiary’s financial institution. More than one intermediary bank may be involved in the process before the money reaches beneficiary’s financial institution.
* SWIFT is a member-owned cooperative established in 1973. It is used by more than 10,000 banking organisations, securities institutions and corporate customers in 212 countries. High levels of confidentiality are imposed and security is reinforced through encryption of messages. SWIFT is also subject to a governance structure and publicly available data retrieval policies that enable SWIFT to meet the security commitments required by users. There are three categorised groups of users: supervised financial institutions, non-supervised entities active in the financial industry and closed user groups/corporate entities. SWIFT users are only able to send financial messages within their user category. For example, the Applicant is only able to send financial messages via SWIFT to other supervised financial institutions.
* Less commonly, IMTs are processed by relying on an ADI’s own commercial arrangements, without any use of the SWIFT network. For example, the Applicant may transfer funds to an offshore branch or subsidiary and that branch or subsidiary could make a payment to a beneficiary’s financial institution within that jurisdiction by means of the local payment and settlement system.

## Relevant privacy principles

### IMTs under the National Privacy Principles (NPPs)

Between 2001 and 12 March 2014, the National Privacy Principles (NPPs) in Schedule 3 of the Privacy Act governed the collection, use, disclosure and other handling of personal information by the Applicant and other ADIs. Relevantly, NPP 9 regulated transborder data flows and permitted an organisation in Australia (or an external territory) to transfer personal information about an individual to someone (other than the organisation or the individual) in a foreign country in limited circumstances, including where:

* the transfer was necessary for the performance of a contract between the individual and the organisation (NPP 9(c)), or
* the transfer was necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party (NPP 9(d)), or
* all of the following apply:
  + the transfer is for the benefit of the individual
  + it is impracticable to obtain the consent of the individual to that transfer
  + if it were practicable to obtain such consent, the individual would likely give it (NPP 9(e)).

Between 2001 and 12 March 2014, the Applicant relied on the NPP 9(d) and NPP 9(e) exceptions to disclose the personal information of beneficiaries to overseas financial institutions when processing IMTs.

### IMTs under the Australian Privacy Principles (APPs)

The Privacy Amendment Act commenced on 12 March 2014 and made changes to the Privacy Act that included a repeal of the NPPs and the commencement of a new set of principles (the APPs) that apply to most Australian and Norfolk Island Government agencies and some private section organisations (known as APP entities), including the Applicant. Relevant to the Application, the changes to the Privacy Act included the following:

* A new APP 8 dealing with cross-border disclosure of personal information to replace NPP 9.
  + APP 8.1 requires an APP entity that discloses personal information to an overseas recipient to take reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to the information, unless an APP 8.2 exception applies.
  + The exceptions set out in APP 8.2 differ from the NPP 9 exceptions. Importantly, APP 8.2 does not cover either of the exceptions set out in NPP 9(d) or (e).
* A new accountability approach dealing with cross-border data flows. As part of this approach, a new section 16C provides that where an APP entity discloses personal information to an overseas recipient, in circumstances where the overseas recipient is not bound by the APPs and an APP 8.2 exception does not apply to the disclosure, the APP entity will be taken to have breached the APPs in instances where the overseas recipient does an act or engages in a practice in relation to that information that would be a breach of the APPs (other than APP 1) if the APPs so applied to that act or practice..

While the changes to the Privacy Act made by the Privacy Amendment Act do not prohibit the processing of IMTs by ADIs, they will:

* require that before processing an IMT, the Applicant and other ADIs take reasonable steps to ensure that the overseas financial institution to which a beneficiary’s personal information is to be disclosed, does not breach the APPs (other than APP 1) in relation to that information
* in some circumstances, make the Applicant and other ADIs accountable for any acts or practices of the overseas financial institution that breach the APPs (other than APP 1) in relation to that information.

## Additional information

The Application that led to the making of TPID 2014-1 and GD 2014-1 is available at: <http://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/public-interest-determinations/ANZ_IMT_PID_application_Feb_2014_redacted.pdf>

The Privacy Commissioner's notice of receipt of the application (required by subsection 74(1) of the Privacy Act) is available at: <http://www.oaic.gov.au/privacy/applying-privacy-law/privacy-registers/public-interest-determinations/>

## Reasons for the decision

### Might the processing of IMTs breach an APP?

#### APP 8

In the Application, the Applicant submitted that the Applicant would be unable to rely on any of the relevant exceptions to APP 8.1 when processing IMTs. The exceptions to APP 8.1 are found in APP 8.2, and relevantly include:

* The Applicant reasonably believes that the overseas financial institution is subject to a law or binding scheme that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the APPs protect the information; and there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme (APP 8.2(a)).
  + The Applicant submitted that it would not be practical for it to obtain up-to-date legal advice on the privacy regimes of every jurisdiction to which IMTs may be sent (which may include any jurisdiction that has a functioning banking system). The Applicant submitted that even if it did obtain such legal advice, those countries which do not have substantially similar privacy schemes and do not allow individuals to take action to enforce protection of their personal information, would fall outside of the APP 8.2(a) exception. This would, the Applicant submitted, result in an inability to send IMTs to beneficiaries in particular countries and likely disadvantage senders, especially those supporting families over long distances.
* The Applicant expressly informs the beneficiary that if they consent to the disclosure of the personal information, APP 8.1 won’t apply to the information, and after being so informed, the beneficiary consents to the disclosure (APP 8.2(b)).
  + The Applicant submitted that its role in the IMT process is limited to collecting the information about the beneficiary from the sender of the IMT. There is no legal (or other) relationship between the Applicant and the beneficiary, and there would not be an opportunity for the Applicant to seek the beneficiary’s consent prior to processing the IMT. Further, due to the large volume of IMTs processed, it would not be feasible for the Applicant to contact each beneficiary across a wide range of jurisdictions to obtain their consent to the Applicant disclosing their personal information..

As the Applicant cannot rely on any of the relevant APP 8.2 exceptions, the Applicant will need to comply with APP 8.1 when processing IMTs and take reasonable steps to ensure that the overseas financial institution receiving the beneficiary’s personal information does not breach the APPs in handling that information.

The Office of the Australian Information Commissioner (OAIC) has issued the [APP guidelines](http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/). Chapter 8 (APP 8) of the APP guidelines states that it is generally expected that to comply with APP 8.1, the relevant APP entity will enter into an enforceable contractual arrangement with an overseas recipient that requires the overseas recipient to handle personal information in accordance with the APPs. However, the APP guidelines acknowledge that whether a contract is required, and the terms of the contract, will depend on the circumstances, including the practicability of taking that step.

The Applicant submitted in the Application that it is not practicable to have enforceable contractual arrangements with every potential overseas financial institution to which the Applicant might disclose the beneficiary’s personal information when processing an IMT in order to require compliance with the APPs. Rather, in the majority of IMTs, the Applicant relies on the relationships created by the SWIFT network. It is not feasible for the Applicant or another ADI to try to alter SWIFT to impose contractual obligations on other SWIFT users to comply with the APPs in relation to the personal information of IMT beneficiaries. In addition, it is unlikely that foreign financial institutions would agree to enter into contracts requiring them to handle personal information in accordance with the APPs given the protections afforded by the SWIFT network.

Although the Applicant takes steps to protect the beneficiary’s information that is sent overseas during the processing of an IMT, (for example, whether the transfer occurs as part of the SWIFT network or outside of this network, there are mechanisms in place to ensure the security and confidentiality of that information), there is uncertainty about whether these steps would satisfy the ‘reasonable steps’ test in APP 8.1.

For this reason, the Privacy Commissioner was satisfied that the Applicant may breach APP 8.1 when disclosing a beneficiary’s personal information to an overseas financial institution during the processing of IMTs.

#### Other APPs

Under subsection 16C(2) of the Privacy Act, when an overseas financial institution, to which the Applicant discloses a beneficiary’s personal information, does an act or engages in a practice that would breach an APP (other than APP 1) in relation to that information, the Applicant will be taken to breach that APP if the overseas financial institution is not bound by the APPs.

The Privacy Commissioner was satisfied that the Applicant may be taken to breach an APP (other than APP 1) as a result of subsection 16C(2).

### Does the public interest in processing IMTs substantially outweigh the public interest in complying with the APPs?

In issuing TPID 2014-1, the Privacy Commissioner took account of the matters raised in the Application. Based on the available evidence presented in the Application, the Privacy Commissioner considered on balance, that the public interest in permitting the relevant acts or practices engaged in during IMT processing substantially outweighs the public interest in adherence to the APPs that might be breached.

The Applicant made a number of arguments in the Application as to why the public interest in processing IMTs substantially outweighs the public interest in complying with APP 8.1, and other APPs in cases where the Applicant might be held accountable for a breach by an overseas financial institution:

* *Public interest benefits associated with adhering to the IMT process in its current form*

There are a number of public interest benefits associated with making IMTs available to Australian ADI customers:

* + IMTs allow individuals to benefit from the global movement of money. They can be used to, for example, allow families to support one another over long distances, and allow private transactions to take place involving parties in different jurisdictions.
  + IMTs provide payment security and transaction certainty. This also assists government to better enforce anti-money laundering and counter-terrorism rules.
  + IMTs are an important element of international financial relations, with SWIFT processing a daily average of 10.3 million payment messages.
  + The IMT process in its current form is one component of the global financial system, and Australia is a significant contributor to that system. Maintaining the certainty, reliability and efficiency of IMT processing by ADIs in Australia serves an important public interest within the context of Australia’s role within the global economy. The Applicant maintained that it would be detrimental for Australia’s reputation as a leading international financial participant if it becomes impracticable for ADIs in Australia to process IMTs.
* *Public benefits associated with adhering to APP 8 during IMT processing*

The Applicant submitted that the main public benefit associated with APP 8 compliance during IMT processing is to ensure the protection of the personal information of beneficiaries.

The Applicant noted that in this respect, personal information is already protected in a number of ways when processing IMTs:

* + Disclosure to an overseas financial institution is within a secure environment. IMTs are processed in a heavily regulated and controlled environment, the basis of which is a trusted network of relationships between financial institutions.
  + The disclosures that do occur as part of the IMT process are the minimum needed to to allow the IMT to be processed.
  + The current IMT process appears a successful and secure means of conducting international money transfers. The Applicant stated that it is not aware of any complaint being made by a beneficiary in relation to the offshore disclosure of their personal information in order to process an IMT.
* *Compliance with APP 8.1 not practicable*

It is not practical for the Applicant to take additional steps to ensure compliance with APP 8.1 and impose contractual obligations on all overseas financial institutions receiving the personal information of IMT beneficiaries in order to comply with the APPs:

* The Applicant already takes steps to ensure the security and confidentiality of information that needs to be sent overseas during IMT processing.
* Obtaining agreement from foreign banks to a separate set of privacy standards to process IMTs would be not only inconvenient, but time-consuming and costly.
* It is unlikely that foreign financial institutions, already operating under their own privacy regimes, would agree to enter into such arrangements.
* Moreover, it would not be practicable for the Applicant to attempt to alter SWIFT to impose these contractual obligations with all overseas SWIFT members. The Applicant has pointed out that the ‘interconnectedness of the global financial system’ means that any change to SWIFT would have significant consequences for the whole financial system.

Without those additional steps there is uncertainty about whether or not the Applicant complies with APP 8.1 because it is not clear that the steps that it does take would be considered ‘reasonable in the circumstances’. This exposes the Applicant to the risk of being held accountable for a breach of the APPs by overseas financial institutions whose acts or practices would breach the APPs if the APPs applied to those acts or practices.

There is a public benefit in providing certainty to the Applicant and its customers that it will not be held to breach the APPs during IMT processing on and from 12 March 2014.

* *APP 8.2 exceptions not available*

Presently, the IMT process provides a simple, secure, cost-effective and reliable means for the global transfer of money, providing benefit to Applicant customers and beneficiaries alike. The APP 8.2 exceptions will not generally be available to the Applicant in the context of the IMT process. The Applicant maintained that this is because the costs and/or delays associated with ensuring compliance with APP 8.2 exceptions would make IMTs prohibitive, impractical and expose ADI customers to risk.

* + Attempts to seek the consent of all beneficiaries (assuming that this was practicable) would result in significant transaction costs for ANZ customers, effectively putting IMTs out of the reach of most Australian ADI customers.
  + The need to contact the beneficiary’s financial institution and/or the beneficiary would result in a significant increase in the time taken to complete the IMT process.
  + Alternatively the need to obtain and maintain up-to-date legal advice on the privacy regimes in every country would be substantial and likely to result in further delays and consequently increased transaction risks for ADI customers (the Applicant noted, as an example, because of exposure to exchange rate movements and because it would be unclear when it would be possible to actually pay the relevant moneys to the beneficiary).
  + A likely consequence of increased costs, delays and decreased transaction certainty in the processing of IMTs is an increasing number of customers relying on less secure and less regulated means of international money transfer, such as informal remittance services.

There would, in this context, be very little public benefit associated with requiring the Applicant to take additional steps to ensure the overseas recipient does not breach the APPs or to rely on any of the APP 8.2 exceptions when processing IMTs.

### Does the application raise issues that require an urgent decision?

The Applicant sought a temporary PID under section 80A of the Privacy Act in order to continue to be able to offer IMTs to its customers without breaching the Privacy Act, while the PID application was under consideration.

The Privacy Commissioner was satisfied that an urgent decision is required because:

* the APPs and subsection 16C(2) commence on 12 March 2014, and absent a PID, the Applicant may breach APP 8, or be taken to breach the other APPs (except of APP 1) if it continues to process IMTs after that date
* due consideration of the Application, including compliance with the required processes in Division 1, Part VI of the Privacy Act and the *Legislative Instruments Act 2003* (Legislative Instruments Act), will require a period of time that extends well beyond 12 March 2014
* a TPID would allow the Applicant to continue to offer, and the Applicant’s customers to continue to enjoy the benefits of, IMTs while the Application is under further consideration.

## Operation

TPID 2014-1 and GD 2014-1 will remain in force for a period of 12 months from the date of commencement, as permitted by subsection 80A(3) unless ceased earlier (see s 80D(2).

TPID 2014-1 applies directly to the Applicant as an APP entity under the Privacy Act.

GD 2014-1 applies to all other authorised deposit-taking institutions within the meaning of the *Banking Act 1959* (ADIs). A list of the ADIs is maintained by the Australian Prudential Regulatory Authority. At the date of this instrument, there are approximately 164 ADIs in Australia.

## Consultation

The Applicant, the Australian Bankers’ Association and the Attorney-General’s Department were consulted in the making of TPID 2014-1 and GD 2014-1. No other entities were consulted.

The Privacy Act does not require consultation to occur prior to the making of a TPID or a determination generalising a TPID. The Privacy Commissioner was satisfied that any further consultation required under section 17 of the Legislative Instruments Actis unnecessary or inappropriate because the TPID is required as a matter of urgency (paragraph 18(2)(b)).

Public consultation on the issues considered in making TPID 2014-1 and GD 2014-1 will occur as the Application is progressed to consider whether further determinations under subsections 72(2) and (4) of the Privacy Act should be made.

**Statement of Compatibility with Human Rights**

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

*Privacy (International Money Transfers) Temporary Public Interest Determination 2014 (No. 1)* (TPID 2014-1) and *Privacy (International Money Transfers) Generalising Determination 2014 (No. 1)* (GD 2014-1)

These Legislative Instruments are 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 Legislative Instruments**

The purpose of TPID 2014-1 and GD 2014-1 is to permit Australia and New Zealand Banking Group Limited (ANZ) and other authorised-deposit taking institutions within the meaning of the *Banking Act 1959* (ADIs) to disclose the personal information of a beneficiary of an international money transfer (IMT) to an overseas financial institution when processing an IMT without breaching the Australian Privacy Principles (APPs), following the commencement of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012.*

The central public interest objective served by TPID 2014-1 and GD 2014-1 is to permit the Applicant and other ADIs to continue to process IMTs, which has benefits for individuals who might send or receive money using IMTs, Australia and its reputation as a participant in the global financial system, and the stability of the global financial system.

**Human rights implications**

The determinations engage 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 and attacks. The Preamble to the Privacy Act makes clear that the legislation was intended to implement, at least in part, Australia’s obligations relating to privacy under the ICCPR.

TPID 2014-1 and GD 2014-1 limit the right against the arbitrary interference with privacy, and advance the right to the protection of the law against such interference, by limiting the application of protections in the Privacy Act in relation to the cross-border disclosure of personal information.

However, the right to privacy is not absolute and there may be circumstances in which the guarantees in article 17 can be outweighed by other considerations. Importantly, the Commissioner must have regard to the objects of the Privacy Act when exercising his functions and powers. These objects include:

* to promote the protection of the privacy of individuals (paragraph 2A(a))
* to recognise that the protection of the privacy of individuals is balanced with the interest of entities in carrying out their functions and activities (paragraph 2A(b))
* to promote responsible and transparent handling of personal information by entities (paragraph 2A(d))
* to facilitate the free flow of information across national borders while ensuring that the privacy of individuals is respected (paragraph 2A(f)).

The Privacy Commissioner was satisfied that the public interest in permitting the acts or practices the subject of TPID 2014-1 and GD 2014-1 substantially outweigh the public interest in adhering to the APPs.

**Conclusion**

It is considered that to the extent that the acts or practices authorised by TPID 2014-1 and GD 2014-1 limit human rights, those limitations are reasonable and proportionate.

Timothy Pilgrim,

Privacy Commissioner