Australian
Privacy
Foundation

p o s t: GPO Box 1196
Sydney NSW 2001

e m a i l: enquiries@privacy.org.au

w e b : www.privacy.org.au

6 July 2006

Ms Karen Curtis
Australian Privacy Commissioner
GPO Box 5218
SYDNEY
NSW 2001

Re: SWIFT – disclosures of Australians' financial information without warrant to the USA

Dear Commissioner,

We are aware that our colleagues from Privacy International wrote to you on 27 June 2006, about the allegations, reported in the media last week, that the US government has covertly accessed records of international financial transactions held by the Society for Worldwide Interbank Financial Telecommunications (SWIFT), which is based in Belgium but has offices in Australia.

We share the concerns expressed by Privacy International.

The allegations

The alleged privacy intrusion will have potentially affected any Australian customers of participating financial institutions making international transactions during the relevant period. This apparently includes at least 11 Australian banks.

We are of course aware that under the Financial Transaction Reports Act 1988, all Australian financial institutions are required to report all International Funds Transfer Instructions (IFTIs), for any amount, to AUSTRAC, where the records are held indefinitely and accessible on-line to more than 30 Commonwealth and State agencies, for a wide range of purposes.

We have previously, and repeatedly, voiced our concern that this reporting regime within Australia is entirely disproportionate to the ostensible objective of the legislation. However these latest allegations suggest personal information about Australians' financial affairs is being transferred unlawfully to the USA, without any oversight by the Australian Government.

The allegations suggest that a large number of transaction records may have been disclosed by SWIFT to US authorities in response to letters, termed "administrative subpoenas", without judicial approval in the USA or any express approval by relevant European authorities, and without the knowledge of the account holders concerned. It has been suggested that these disclosures may have been unlawful, under the laws of various jurisdictions.

The figures cited by Privacy International from the SWIFT Annual Report suggest that a very large number of Australians, as customers of many Australian financial institutions, may have been affected. We submit that Australians who have made overseas transactions in the recent past have a legitimate interest in knowing whether their records have been disclosed and if so whether that disclosure was lawful.

We submit that the fact that the same information about transactions will have been reported to AUSTRAC does not in any way diminish the seriousness of the allegations.

Coverage of complaint under the National Privacy Principles

Most if not all of the participating Australian financial institutions would be 'organisations' subject to the National Privacy Principles of the Privacy Act (as well as to obligations of confidence – an important issue which we do not explore further in this letter). It should be relatively easy to identify which Australian organisations have used SWIFT services.

Notification of disclosures

Whether or not the organisations concerned have notified customers transferring funds overseas of the reporting to AUSTRAC (we have our doubts about the level of compliance with NPP 1.3 in this respect), it seems unlikely that they will have notified them of the possibility of disclosure by SWIFT to US authorities. If the Australian organisations were aware of the disclosures, then we suggest that there is an issue of compliance with NPP 1.3 (Collection Notification).

We submit that you should ascertain from the organisations concerned whether they were aware of the disclosures from SWIFT to the USA, and if so how they consider they have complied with NPP 1.3 (or NPP 1.5 with respect to notification of indirect collections).

Legality of disclosures

There are also issues of compliance with NPPs 2 and 9, concerning the lawfulness of any disclosures, to SWIFT and beyond.

Under NPP 2 (Use and Disclosure), disclosures of this character would presumably have to meet the terms of exceptions (g) (the use or disclosure is required or

authorised by or under law) or (h) (the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body).

If the organisations concerned were aware of the disclosures from SWIFT to the USA, did they satisfy themselves that one of these exceptions applied?

We submit that you should ascertain from the organisations concerned, if they were aware of the disclosures, what authority under NPP 2 they consider provided for the disclosures.

Because transfers of personal information overseas to SWIFT are concerned, Australian organisations also have to comply with NPP 9 (Transborder Data Flows). We assume that financial institutions would rely either on the existence of privacy laws in the other countries involved (especially Belgium), or on contracts with the other parties involved in transactions, including SWIFT, or on consent from their customers. However it is unclear whether reliance on say Belgian data protection laws is sufficient, if there is evidence that those laws have not been used to prevent further disclosures outside the EU's strict data protection regime, to the USA.

We submit that it you should ascertain from the organisations concerned the basis of their compliance with NPP 9.

Data security

There are also issues of compliance with NPP 4 in relation to data security, whether or not the organisations concerned were aware of the alleged disclosures.

We submit that you should ascertain how the organisations concerned consider that they have complied with NPP 4 in respect of personal information sent through SWIFT. If they were not aware of the disclosures to the USA, then what steps have they taken, or are taking since they became aware of the allegations, to prevent any further unauthorised disclosures.

Investigation requested

Given the systemic character of the allegations raised, we hope you will agree that this matter is best dealt with, at least initially, by means of an 'own-motion' investigation without anyone having to bring individual or representative complaints. This does not limit the possibility of such complaints in future, and you may well have already received some. We understand that you do have the discretion, used in the past, to suspend consideration of individual complaints pending the outcome of an own-motion investigation.

In order to provide the answers to the questions posed above, we therefore request that you undertake a comprehensive own-motion investigation into Australian financial organisations' compliance with the NPPs in relation to these allegations. It may be that some of the questions can be answered collectively by industry organisations, or by representative organisations on behalf of all of those concerned.

This might help to limit the resources required and result in a more efficient and speedy investigation.

We encourage you to liaise in the course of your investigation with your counterpart privacy or data protection regulators in the other jurisdictions concerned, and especially those of Belgium and the European Union.

We further submit that you should consider whether this incident lends weight to the proposal, which we and others have canvassed, for mandatory notification of individuals affected by instances of unauthorised disclosure or loss of personal information. If so, we urge you to make representations to government for urgent legislative amendments to introduce such a requirement.

Finally, we request that you seek confirmation from AUSTRAC that the IFTI information it holds has not been, and will not be, made available to US authorities either directly, or indirectly through AUSTRAC's partner agencies. If it has, then the public is entitled to know the extent of any such disclosures and the legislative authority for them.

Yours sincerely

Anna Johnston
Chair, Australian Privacy Foundation

Phone: (02) 9432 0320

About the Australian Privacy Foundation

The Australian Privacy Foundation is the leading non-governmental organisation dedicated to protecting the privacy rights of Australians. We aim to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians.

Since 1987 the Australian Privacy Foundation has led the defence of the rights of individuals to control their personal information and to be free of excessive intrusions. We use the Australian Privacy Charter as a benchmark against which laws, regulations and privacy invasive initiatives can be assessed.

For further information about us see www.privacy.org.au