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

12 October 2006

Mr Timothy Pilgrim
Deputy Privacy Commissioner
GPO Box 5218
SYDNEY NSW 2001

Re: Breach of Privacy Act by Australian financial institutions

Dear Mr Pilgrim,

I refer to your letters dated 22 September and 12 October 2006, in response to our concerns about the disclosure of personal information by the Society for Worldwide Interbank Financial Telecommunications (SWIFT), to US government agencies.

We understand you initially focussed on the issue of whether SWIFT organisation itself was subject to the Privacy Act jurisdiction, and that you believe that it is not.

We also understand and appreciate that, following further discussions on 11 October, you will now turn to investigating our allegations of non-compliance by Australian financial institutions.

We are therefore taking this opportunity to reformulate our allegations based on new information and further analysis, in order to assist in your investigations.

Our contention is that the disclosures by SWIFT raise questions of compliance with the National Privacy Principles by all Australian financial institutions who are users of the SWIFT network, rather than non-compliance by SWIFT itself.

According to SWIFT's Annual Report for 2005, 11 Australian banks and 88 'institutions' sent messages over the SWIFTNet FIN Service and there were more than 3 million Australian messages sent over the SWIFTNet InterAct service. We have specifically identified NPPs 1, 4 & 9 as those which might have been breached if information about the transactions of Australian clients was included in the information disclosed by SWIFT during the relevant period. Our specific allegations are set out below.

Given the difficulty of individual Australians establishing whether their personal information has been disclosed, and the likelihood that if it has it would be a widespread systemic issue, we suggest that the obvious response to these serious allegations would be an own-motion investigation by your office, firstly to establish by enquiry to major financial institutions (or perhaps via an appropriate industry body) the extent of their involvement in SWIFT and secondly to seek the response of relevant institutions to the questions about NPP compliance (see below).

It will be very disappointing, and very inefficient for all concerned, if we have to go down the path of individual complaints, or even a representative complaint, to achieve investigation of what is clearly a significant systemic compliance issue.

We also 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 note that the Belgian Commissioner has already found breaches of their Data Protection Law, and that other European Commissioners are also undertaking investigations. We note and welcome your intention to monitor the progress of the investigation by the EU Article 29 Working Party. However, we do not see this as in any way an adequate substitute for investigation by your office to ensure compliance by Australian organisations with the Privacy Act 1988.

Compliance with the National Privacy Principles

We allege that Australian financial institutions, including the 'big four' banks Westpac, ANZ, NAB, and the Commonwealth Bank, may have breached the following National Privacy Principles 1, 4 and 9.

We request that you consider separately the compliance issues in relation to

(a) the period before the New York Times article (23 June 2006) and subsequent publicity, when Australian financial institutions may not have been aware of bulk disclosures by SWIFT to US government agencies,

(b) the period since that publicity, when major institutions at least can be assumed to have become aware of the disclosures and subsequent controversy, and

(c) the period since it has become clear that there may have been breaches of the data protection laws of some jurisdictions to which SWIFT is subject.

We suggest that it is more likely that breaches of the relevant Principles can be established in the second and third periods, but that your investigation should consider all three periods where relevant (as indicated below).

The Principles which we believe may have been breached are as follows:

NPP 1, Collection

- by failing to inform customers using SWIFT services about the potential disclosure of their personal financial information to SWIFT, being 'an organisation to which the organisation usually discloses information of that kind' (NPP 1.3). This issue relates

to periods (a), (b) and (c), but is now of more serious import in (b) and (c). At the very least, Australians should be aware that information about their overseas transfers of funds are handled by SWIFT. They can then take their own steps to find out the implications of this.

NPP 9, Transborder data flows

- by continuing to transfer (via SWIFT) customers' personal information to SWIFT's operations located both in Europe and in the United States, in circumstances where none of the exceptions to NPP 9 apply. Specifically, the following exceptions may not apply in the current circumstances where organisations are aware of the disclosures by SWIFT to US government agencies (period (b)), and more particularly aware of the findings of at least one European data protection agency that SWIFT has breached the law of that jurisdiction (period (c)) :

- Exception (a) "the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the NPPs."

    - In respect of the transfer to the SWIFT Processing centre in Europe, Australian organisations may reasonably conclude that European Data Protection laws satisfy this exception, any failure of European Commissioners to actually prevent unlawful disclosures would suggest they are not 'effectively upheld'. While we may not know if this is the case for some time, the uncertainty must surely cast doubt on reliance on this exception.

    - In respect of SWIFT transfers to the SWIFT Processing centre in the USA, we cannot see how any organisation could reasonably rely on this exception. There are to our knowledge no US privacy laws applying to SWIFT or other potential US recipients of SWIFT data that are 'substantially similar' to the NPPs, and there has been no suggestion that SWIFT is subject to a 'binding scheme' (whether a 'safe harbour' agreement or otherwise) or contract that achieves this objective.

- Exception (b) "the individual consents to the transfer", or alternatively Exception (e), which we paraphrase as "impracticable to seek consent but it would likely be given"

    - For both these exceptions, the actual or assumed consent must be free and informed, and it cannot reasonably be said to be informed if the individual has not been notified about such a controversial 'consequential' disclosure as the SWIFT disclosure to US authorities. It also appears that Australian banks may not have been aware of the nature of the disclosures and the limited initial control over their 'purpose', so we would question how could their customers (who have no independent relationship with SWIFT) have known enough to give informed consent?

- (c) the transfer is necessary for the performance of a contract between the individual and the organisation …"

    - This seems on the face of it to be the most likely basis for compliance with NPP 9, but we question whether it should be interpreted as a stand-alone criterion independent of consideration of the objectives of NPP 9. We suggest it should not be able to be relied on as a basis for overseas transfer in circumstances where there is knowledge that the personal information will be used in ways that would contravene one or more of the NPPs, if such uses were to take place in Australia.

NPP 4, Security

– by failing to take reasonable steps to protect customers' personal information from disclosure through SWIFT to US agencies, which disclosure is allegedly unlawful under the laws of at least some of the jurisdictions to which SWIFT is subject.

It may be that investigation would expose further or different compliance issues. Equally, such an investigation may expose deficiencies in the NPPs and the Privacy Act where personal information is being exported under circumstances where international systems for handling personal information expose the personal data of Australians to levels of risk known to institutional participants, but not to the individuals concerned.

We emphasise that each of the above breaches will potentially have been committed by every Australian organisation using the SWIFT network.

To the extent that SWIFT may still be disclosing information to US government agencies under the reported arrangements, Australian organisations affected will remain in breach and we suggest that it would be appropriate for you to consider the use of the injunction provisions of the Privacy Act 1988 (s.98) to immediately bring them into compliance.

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 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 International Funds Transfer Instruction (IFTI) information it holds (which we understand to be all such transactions, however small, held indefinitely) 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.

We note that your letters are labelled IN CONFIDENCE. We assume this is based on the provision in s.43(2) that "an investigation under this Division shall be

conducted in private …", a provision that applies to both complaint and own-motion investigations. We take this provision to be designed primarily to protect complainants' privacy, and also to facilitate the Commissioner's efforts to conciliate complaints. We do not however see s.43(2) as entitling the Commissioner to preclude complainants making a copy of their complaint public. We intend to do so in this case.

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