



Australian Government
Office of the Privacy Commissioner

Our reference: 2000-449-01

Mr Michael Funston
Public Affairs
Abacus – Australian Mutuals
GPO Box 4720
Sydney NSW 2001
By email: mfunston@abacus.org.au

Level 8 Piccadilly Tower
133 Castlereagh Street
Sydney NSW 2000
GPO Box 5218
Sydney NSW 2001

P +61 2 9284 9800
F +61 2 9284 9666
privacy@privacy.gov.au

Enquiries 1300 363 992
TTY 1800 620 241
www.privacy.gov.au
ABN 13 152 473 225

Dear Mr Funston

CONSULTATION DRAFT OF ABACUS AUSTRALIAN MUTUALS – CODE OF PRACTICE

I refer to your letter of 31 October 2007, inviting the Office of the Privacy Commissioner ('the Office') to comment on Abacus – Australian Mutual's ('Abacus') draft *Code of Practice* ('the draft Code'). I apologise that the Office was not able to meet your proposed deadline for submissions and appreciate Abacus accepting these late comments.

The comments provided below are intended as general advice on the draft Code as it may relate to the privacy of individual's personal information, and is not legal advice. If the Office received a complaint about a matter covered by the Code of the Practice, the matter would be investigated according to its own facts.

About the Office

The Office is an independent statutory body whose purpose it is to promote and protect privacy in Australia. The Office has responsibility for the protection of individuals' personal information that is handled by Australian and ACT government agencies, and personal information held by all large private sector organisations, health service providers and some small businesses. The *Privacy Act 1988* (the Privacy Act) regulates how these agencies and organisations handle personal information.

Relevantly, the National Privacy Principles contained in schedule 2 of the Privacy Act will generally apply to any of Abacus's members with an annual turnover of more than \$3 million. While it may be unlikely that any of your members would have a turnover of \$3 million or less, the Office also notes that such businesses will be covered by the NPPs in regard to personal information collected pursuant to the *Anti-money and Counter-Terrorism Financing Act* (2006). Information on how the Privacy Act interacts with this legislation is available from the Office's dedicated AML/CTF webpage at <http://www.privacy.gov.au/business/aml/index.html>.

In addition, Part IIIA, concerning credit reporting, will likely apply to all mutual building societies and credit unions.

Community attitudes to financial information

The Office welcomes the opportunity to contribute to the development of the draft Code. The Office, through ongoing research on community attitudes, has consistently found that individuals believe that their personal financial information is especially

sensitive.¹ In the Office’s view, organisations that commit to meeting their privacy obligations in an active and robust manner are more likely to engender the trust and confidence of their customers. Accordingly, exercising care in how personal financial information is handled will, we believe, benefit both the individual and the business.

The Office notes the clear statement that the draft Code, if adopted, would not purport to vary any obligations your members may have under law, expressly including the Privacy Act. The Office welcomes this recognition in the draft Code.

Safe guards for loan guarantors

The Office has some concerns regarding draft clause 9.7.

As you are likely aware, Part IIIA of the Privacy Act was enacted in 1990 to regulate the practices of credit reporting agencies and credit providers in relation to personal credit information. Part IIIA restricts access to the consumer credit reporting system by providing prescriptive regulation and includes criminal sanctions for non-compliance.

Section 18N prohibits credit providers disclosing credit worthiness information to “another person for any purpose” unless a prescribed exception applies. One of these exceptions is provided in section 18(N)(1)(bh), which permits disclosures:

for the purpose of that person considering whether to offer to act as guarantor in respect of, or to offer property as security for:

- (i) a loan given by the credit provider to the individual concerned; or
- (ii) a loan for which the individual concerned has applied to the credit provider;

and the individual has specifically agreed to the disclosure of the report or information to any such person for that purpose

However, it is unclear whether draft clause 9.7 accurately reflects this provision. In particular, it is unclear what types of personal information are intended to be captured in the third dot point (permitting ‘any other matter relevant to the borrower or the loan facility to be secured’) and whether this dot point could be interpreted as permitting types of information to be disclosed that go beyond the intent of section 18(N)(1)(bh). The Office suggests that this dot point should usefully be clarified or omitted.

Provision of statements and notice electronically

The Office suggests that draft clause 15 could usefully refer to the importance of ensuring that electronic communications are through appropriately secure media. NPP 4 requires that organisations take reasonable steps to protect personal information from unauthorised access, modification or disclosure. It is likely to accord with community expectations for personal financial information to be afforded robust security protections, including where it is transmitted electronically to the consumer, such as by applying encryption techniques.

Additional copies of documents and statements

Section 16 refers to the additional copies of documents and statements that an Abacus member will provide to clients under the Code. The Privacy Act requires organisations to provide individuals with access to their personal information. The

¹ As reported in various community attitude research projects undertaken by the Office – see, <http://www.privacy.gov.au/publications/#R>.

provision of copies of documents and statements would be considered to be access to personal information. The Office suggests that Abacus consider including a reference to clause 21.3, which briefly outlines Privacy Act access obligations.

Account security and security breaches

NPP 4 requires organisations to “take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure”, as well as to destroy or permanently de-identify personal information that is no longer required.

While the Office generally welcomes the discussion of information security provided in draft clause 17, you may wish to consider including a reference in section 17 that reflects these NPP 4 obligations. The Office suggests the following clause:

“In accordance with our obligations under the *Privacy Act 1988*, we will take reasonable steps to protect the personal information that we hold from misuse and loss and from unauthorised access, modification and disclosure. We are committed to destroying or permanently de-identifying personal information if it is no longer needed for any purpose for which the information was collected.”

Privacy and confidentiality

The Office supports Abacus’ initiative to promote best practice in regard to privacy. As a reflection of this, the Office suggests the following minor amendments as a means of enhancing the privacy practice of Abacus members.

Contractors

At times, organisations may contract out (outsource) a function that requires a contractor to collect and handle personal information on behalf of the organisation. The Office has noted that such practices have, on occasion, been a cause of concern in the community, such as where information is sent to off-shore contractors for processing.

The Office suggests that it would be good privacy practice, and promote community confidence, for the draft Code to establish a requirement that members ensure any contracts entered into include clauses requiring the contractor to handle personal information in a manner consistent with the Privacy Act.

Further information on the role of contractors under the Privacy Act is available in Information Sheet 8, available from the Office’s website at http://www.privacy.gov.au/publications/IS8_01.html.

Privacy Impact Assessments

As noted above, the privacy of personal financial information is of keen interest to many individuals in the community. The Office encourages organisations that are considering proposals that involve the handling of large amounts of personal information or personal information is particularly sensitive in nature, to consider conducting a comprehensive PIA at the initial proposal stage. Given the sensitivity of personal financial information and the importance of maintaining consumer confidence, the benefits of such an assessment are likely to be heightened in the finance sector.

The *Privacy Impact Assessment Guide* ('PIA Guide') released by the Office in August 2006 is intended to assist Australian and ACT Government agencies in determining the impact new proposals could have on privacy. While the PIA Guide is targeted at government agencies, the core principles can be readily applied to and used by private sector organisations.

Accordingly, you may want to consider including a reference to PIAs within the code of practice. The PIA Guide may assist Abacus members to integrate privacy into the risk management plan of their organisations by working through some practical steps that will:

- identify and define the project scope and aims;
- describe and map the flows of personal information within the project;
- identify and analyse how the project may impact on privacy; and
- consider options to improve privacy outcomes.

A PIA can be produced summarising the privacy information and making recommendations about how the privacy impacts and project aims can be successfully managed. A copy of the PIA Guide is attached and is also available at <http://www.privacy.gov.au/publications/PIA06.doc>.

Alternatively, if Abacus chooses not to include express reference to PIAs in the Code of Practice, the Office would nonetheless encourage their promotion in the sector. We would be pleased to discuss further how the Office could assist in this process.

The Office hopes that Abacus finds these comments useful.

If you have any further enquiries, the contact officer is Linda King, who may be contacted on (02) 9284 9820, or LindaKing@privacy.gov.au.

Yours sincerely

A handwritten signature in black ink, appearing to read 'MH', with a large, sweeping flourish extending to the left.

Mark Hummerston
Acting Deputy Privacy Commissioner
16 January 2008