



Abacus
Australian Mutuals

Association of Building Societies and Credit Unions

28 July 2010

Ms Christine McDonald
Committee Secretary
Senate Standing Committee on Finance and Public Administration
Email: fpa.sen@aph.gov.au

Dear Ms McDonald

Inquiry into Exposure Drafts of Australian Privacy Amendment Legislation

Thank you for the opportunity to make this submission into the Exposure Drafts of Australian Privacy Amendment Legislation.

Abacus – Australian Mutuals is the industry body for customer-owned financial institutions, representing 104 credit unions, 9 mutual building societies and 25 friendly societies. Our member institutions serve 6 million Australians and hold total assets of \$70 billion.

Abacus is a member of the Australasian Retail Credit Association. Abacus members collect, hold, and use a variety of personal information of their members. This information is often of an extremely sensitive nature, relating to their financial position, their health status, and their employment and residential arrangements, amongst other details.

For the purposes of this submission, we have restricted our comments to issues with Australian Privacy Principles (APP) of relevance to Abacus members.

Australian Privacy Principle 2: Anonymity & pseudonymity

Abacus supports the inclusion of an explicit acknowledgement that institutions can decline to deal anonymously with individuals on banking matters, particularly with reference to the operation of Anti-Money Laundering and Counter Terrorism Financing (AML/CTF) responsibilities under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*. We believe that this APP will provide greater clarity for our institutions when dealing with members.

Australian Privacy Principle 4: Receiving unsolicited personal information

APP4 requires the destruction of unsolicited personal information that is not required. Abacus is concerned that this requirement may create some very difficult practical issues and unintended consequences for our members in practice. For example, if a customer (or another member of that household) discloses extensive personal information that is not required by the Abacus member during a phone call where other *required information* is collected, then a record of the *whole phone call* may need to be destroyed if the not-required information is unable to be separated

from the required information. Abacus proposes that this APP is reworded (or at least interpreted) to say that if information can't reasonably be disposed of, steps must be taken to ensure it is not used, which would thereby achieve the same effective result for the customer.

Additionally, Abacus suggests that in order to clarify the meaning of "no longer personal information" at APP4.4(b) the following should be inserted at the end of this sub-clause "(for example, by taking steps to remove any reference to the individual to whom the information relates)" (see p10 of the Companion Guide). This phrase simplifies the meaning of this clause, and for clarity we propose this simple drafting amendment.

Australian Privacy Principle 5: Notification of the collection of personal information

Abacus is concerned that the operation of APP5 could be inconsistent with AML/CTF Act tipping off obligations. Section 123 of the AML/CTF Act requires that an institution must not disclose to any non-AUSTRAC person that a suspect matter report (SUSMR) has been lodged (or that a suspicion has been formed that a SUSMR needs to be lodged). There may be limited cases where APP5 could create problems under this requirement, and for the purpose of clarification Abacus proposes an amendment to APP5 to explicitly note that a tipping off issue overrides any of the requirements to notify collection of personal information.

APP5 has also omitted the exceptions that appeared in NPP1.5. Abacus proposes that the exceptions are reintroduced, namely the obligation to notify the affected individual of the collection of personal information when the notification will pose a serious threat to the life or health of any individual. This exemption has been utilised by Abacus members when they have needed to collect personal information from third parties (e.g. spouse) when dealing with violent members, and we believe that there is a good public policy foundation to continue this exemption, without any corresponding public detriment.

Australian Privacy Principle 7: Direct Marketing

Abacus is concerned that the wording of APP7.6 could have unintended consequences. Whilst the objective of this clause is likely to be that the requirements of the *Spam Act 2003* and the *Do Not Call Register Act 2006* override anything in APP7, another interpretation seems to imply that APP7 won't apply at all if those Acts apply.

Australian Privacy Principle 12: Access to personal information

Abacus notes that there is an amendment between National Privacy Principle 6.3 and APP12.5 that places an additional obligation on an entity. An entity that refuses access for one of the valid reasons "must take such steps (if any) as are reasonable in the circumstances to give access to the information in a way that meets the needs of the entity and the individual." This compares with the current requirement that the entity "must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties"

(which is mirrored in new APP12.6). Abacus questions the need for imposing this extra requirement, particularly given the fact that the listed exceptions to access are well founded.

Please contact me on 02 8299 9053, or Matt Gijselman from Abacus Public Affairs on 02 8299 9048 or email mgijselman@abacus.org.au, to discuss any aspect of this submission.

Yours sincerely

MARK DEGOTARDI
Head of Public Affairs