Level 11, 35 Clarence St
Sydney NSW 2000

GPO Box 4686
Sydney NSW 2001

TEL 02 8035 8400
FAX 02 9262 1040

Abacus
Australian Mutuals

21 June 2013

Tim Bryant
Inquiry Secretary
Senate Standing Committee on Legal and Constitutional Affairs
Parliament House
Canberra

Sent via: legcon.sen@aph.gov.au

Dear Mr Bryant

Privacy Amendment (Privacy Alerts) Bill 2013

We appreciate the opportunity to contribute to the Committee's inquiry into the Privacy Alerts Bill (the Bill).

Abacus is the industry association for Australia's mutual banking institutions, representing 85 credit unions, seven mutual building societies and nine mutual banks. Our members are Authorised Deposit-taking Institutions (ADIs) regulated by APRA under the *Banking Act 1959*. Our members also hold AFS Licences and are licensed under the consumer credit legislation. Abacus members provide the full range of retail banking services and products to more than 4.5 million customers.

The customer owned banking sector puts its customers first. Accordingly, the secure and appropriate handling of a customer's personal information, including credit data, is extremely important for our members. The customer owned banking sector has an excellent record of protecting personal information and we consistently record market-leading customer satisfaction ratings in independent surveys.

Whilst we understand the Government's desire to ensure appropriate handling of customer information, no case has been made to rush the introduction of mandatory breach reporting laws.

We agree that mandatory breach reporting has been under consideration for some time and is widely supported in-principle, but the process of drafting and introducing the Bill and the associated consultation process is unsatisfactory.

The regulatory cost burden for Abacus members and other entities imposed by the Bill includes creating notification methods, changes to compliance systems and processes and increased insurance and legal costs. Rushing in the new regime will unnecessarily increase these costs.

Our concerns are:

- The draft Bill was not made available to all stakeholders and the Bill is subject to a highly abridged Committee inquiry;
- There is uncertainty about various definitions in the Bill; and
- There is significant doubt that that the Office of Australian Information Commissioner will be able to provide entities with the necessary guidance by March 2014.

We recommend that the Bill's commencement date should be March 2015, 12 months later than currently proposed.

Definitions

There is uncertainty associated with a number of the definitions outlined in the Bill.

The Bill addresses the requirement for organisations to notify affected individuals and the Commissioner when a data breach results in "real risk" of "serious harm". The application of these terms will largely rely on an organisation's interpretation of them in the context of a data breach. Guidance about key definitions is required from the OAIC, so that the risk of over-notification and "notification fatigue" is minimised.

It is important for affected organisations to better understand what factors they can and should take into account when determining what constitutes real risk of serious harm. Allowing organisations to take a risk-based approach to this assessment will ensure that important customer protection principles are met without unnecessarily incurring compliance costs for ineffective or excessive notification purposes.

Guidance is also needed on the obligation to notify "as soon as practicable".

There is considerable uncertainty, and potentially significant reputational risk and confidence impacts, arising from the provisions relating to "general publication conditions". These conditions are to be subject to regulations but there is no indication about the nature of the regulations.

OAIC resourcing & capacity

It is important that these reforms, should they be implemented, achieve the outcomes intended by the Government.

There is a risk of what the Government has termed "notification fatigue" in the Explanatory Memorandum. The suite of privacy reforms the Government intends to have implemented in March 2014 will include the possibility for civil penalties to apply to organisations that do not adhere to the notification laws. As such there is a significant risk that organisations will over-notify, causing resourcing implications for both organisations and the OAIC.

The privacy alerts regime comes in addition to significant changes to the privacy regime commencing in March 2014.

The Explanatory Memorandum notes that the OAIC will have a significant workload in both the lead up to and commencement of the new privacy reforms in March 2014 and that this may impact on its ability to produce guidance material pre-commencement.

We understand that the OAIC is already stretched in its capacity to handle the increased workload. The reforms proposed in the Privacy Alerts Bill will further add to the duties of the OAIC and it is unclear how the Government intends to support the OAIC in doing this.

Post-implementation review
Abacus recommends that the Committee supports a review of the effectiveness and operation of the privacy alerts regime 12 months after commencement. Under our recommended timetable, the review would be undertaken in 2016.

Yours sincerely

Luke Lawler
Senior Manager, Public Affairs