Australian Finance Conference Level 8, 39 Martin Place, Sydney 2000 GPO Box 1595, Sydney 2001
ABN 13 000 493 907 Telephone: (02) 9231-5877 Facsimile: (02) 9232-5647 e-mail: afc@afc.asn.au

20 June 2013

Ms Julie Dennett
Committee Secretary
Senate Standing Committee on Legal and Constitutional Affairs
PO Box 6100 Parliament House
Canberra ACT 2600 By email: legcon.sen@aph.gov.au

Dear Ms Dennett,

PRIVACY AMENDMENT (PRIVACY ALERTS) BILL 2013 – AFC COMMENTS

The Australian Finance Conference (AFC) appreciates the opportunity to provide feedback for the Committee's consideration on its inquiry and report on the Privacy Amendment (Privacy Alerts) Bill 2013 (the Alerts Bill).

Background
By way of background, AFC membership includes a range of credit providers, financiers, receivables managers and the three Australian consumer credit reporting agencies. AFC member companies are involved in the full range of lending financial services in both the consumer and commercial markets. The handling of personal information of customers and others is a critical component of our Members' business.

Consequently, embedded within their organisations is a culture of privacy compliance. This reflects management of regulatory risk (eg from compliance obligations arising under the Privacy Act, National Consumer Credit Protection Laws, Voluntary Codes and common law "breach of confidentiality" obligations). For, AFC Members operating in the consumer credit market, potential loss of their Australian Credit License for non-compliance with their general conduct obligations (which includes non-compliance with the credit reporting provisions of the privacy legislation) with the resultant inability to continue in the consumer credit market acts as a significant incentive to ensure compliance.

More importantly, however, the compliance culture reflects acknowledgment by AFC Members that the personal information of both external stakeholders (eg customers; shareholders) and internal stakeholders (eg employees) is a critical asset to their businesses and consequently should be afforded the highest protection. Management of reputational risk equally drives compliance in this regard.

Our consideration of the Alerts Bill has also taken note of the extensive privacy reform process that has preceded the introduction into the Senate of the Alerts Bill, including the recent passage in later 2012 of amendments to the Privacy Act to enhance the consumer protections contained within it. The AFC has been pleased to have participated in that process. Also relevant to this matter, the AFC has provided input into the development by the Privacy Commissioner's of the *Data Breach Notification: A Guide to Handling Personal Information Security Breaches* and the review by the Australian Law Reform Commission

(ALRC) of the Australian privacy laws which culminated in the issue of *Report 108: FYI: Australian Privacy Law & Practice* and, in particular, Recommendation 51-1.

Committee Focus
We understand that the reasons for the referral and principal issues for consideration by the Committee are:

- Regulatory burden on business;
- Interoperability of the Bill with voluntary codes currently being prepared;
- Adequacy of the Privacy Commissioner's resources to administer the regime and to deal with current responsibilities in code formulation;
- Status of code formulation;
- Progress of a consumer education program for the new privacy regime;
- Extent of the regime established by the Bill that is to be contained in Regulations.

It is with the above background and parameters underpinning the Inquiry that we provide the following comments also appreciating the tight-timeframe for the Committee to report.

AFC Comments
The AFC shares Parliament's objective of achieving a regulated information-handling system that "*appropriately balances the protection of the privacy of the individual's personal information with the interests of industry participants in carrying out their functions or activities; to facilitate an efficient credit reporting system while ensuring that the privacy of individuals is respected"* including through "*responsible and transparent information-handling practices*" supported by a "*complaints process to address allegations of privacy interferences" (Privacy Act as amended by the Privacy Protection (Enhancing Privacy Protections Act 2012* - s. 2A Objects of this Act).

In our view, however, the proposed scheme contained in the Alerts Bill will have significant impact for the financial services sector given its coverage includes APP regulated entities, credit providers and TFN recipients. While the compliance obligations proposed are similar, it will nevertheless require an AFC Member to consider the potential impacts and design a compliance framework that deals with each circumstance covered. In addition, we would submit that financial service providers who handle considerable data, and need to hold it for long periods of time, will potentially incur greater costs when compared with other industries where data-handling may not be as significant in terms of day to day operations.

As noted in a range of submissions, including to this Committee in response to earlier inquiries, we re-iterate our concerns that since its inception in 1958, the AFC has never been confronted with the requirement to revisit and respond to such a broad range of fundamental policy positions that have underpinned the regulation of our Members and the financial services industry broadly as it has in the last 24 months. This consideration is being driven by the current reform agenda of the Commonwealth Government. The outcome has been change in the regulatory framework that requires management by our Members.

While recognising the importance of consultation on mandatory data breach reporting, the reform environment in which the consultation is being conducted means AFC Members have limited ability to, at this time, devote the resources to fully consider and provide significant operational detail based on the framework outlined in the Alerts Bill. Analysis to date has identified a fundamental concern with the Alerts Bill, namely:

- the difficulty of considering the potential impacts of a model in which the actual parameters of its operation can be heavily influenced via the Government relying an regulation-making powers to prescribe additional components. For example, sections 26X(1)(d)(ii), 26X(2)(d)(ii), 26X(2)(g)(ii); 26Y(1)(d)(ii),; 26Y(1)(g)(ii);

26Z(1)(d)(ii), 26Z(2)(d)(ii), 26ZA(1)(d)(ii) and 26ZA(2)(d)(ii) all provide a notification may be required if information of a type specified in the regulations is involved, even if there is no real risk of serious harm to an individual. We acknowledge that this may be a drafting protocol to future-proof the regulatory model. However, the absence of clear intention by the Government in relation to its reliance on the powers provided in the short-term, makes assessment of questions of potential impact difficult. The **AFC recommends** that in preference to a process that relies on a regulation, that the Government policy and framework should be contained in the substantive primary legislative amendments of the Alerts Bill.

On a broader level, the AFC is not aware of evidence to substantiate regulatory or market failure that creates consumer protection risk that would justify additional legislation. As noted earlier, safe and secure data handling is embedded within the compliance culture of AFC Members for regulatory risk, customer relations, corporate governance and commercial reasons.

In our view, the current commercial and regulatory risk management imperatives that drive compliance culture for AFC members in data management act as a sufficient inhibitor to privacy breaches. In the experience of AFC members, breaches of customer privacy through mismanagement of personal information are generally a human failing through inadvertence or negligence (eg failure to follow company policies and procedures or abuse of process by third parties) rather than an intentional or reckless action indicative of a regulatory or systemic-compliance failure by the regulated entity. The drive to avoid adverse media attention as a result of inappropriate data handling is also a significant deterrent factor for AFC Members. The combination of risk provides an adequate and effective basis for a compliance framework to be central to our Members operations, (including for the effective security and destruction of data), and to deter or incentivise AFC Members from engaging in inappropriate data handling.

The statutory obligations contained within the Privacy Act to secure and destroy data, (together with those relevant to other stages of information handling by AFC Members), are currently the subject of extensive reform through the imminent enactment of the Government's first stage response to the ALRC Report recommendations; namely the enactment of the Privacy Protection (Enhancing Privacy Protections) Act 2012.

The amendments include enhanced powers of the Privacy Commissioner and avenues for court action (including significant pecuniary penalties and opportunity for compensation) to address mishandling of personal information by regulated entities including AFC Members. These initiatives will have a dual consumer protection benefit of enhancing the ability of the Commissioner to champion the data protection rights and pursue remedies on behalf of an individual in relation to regulated entities, including AFC Members, and add further incentive to our Members and other regulated entities to adopt processes and policies in compliance with the reformed Privacy Act.

Further, in parallel with the mandated obligations, the self-regulatory or voluntary process for breach notification outlined in guidance issued in 2008 by the Privacy Commissioner (and updated in 2012) is, in the view of AFC Members, effective. It reflects the outcome of extensive stakeholder consultation that ensured a process that could be efficiently adopted in a manner that achieved its underlying consumer protection outcome. In addition, regulated entities appear to be utilising the process based on data breach statistics provided in the Australian Information Commissioner's Annual Reports. Of note, contrary to the Government's concern that risk of breach may be on the rise in practice, the statistics of

reported breach in the Commissioner's 2011/12 Report shows an 18% decrease of data breach notifications in comparison with the previous year.

The AFC also notes that the Commissioner has been active in utilising his existing power under the Privacy Act to undertake own motion investigations (eg in the matter of Sony PlayStation Network / Qriocity) to determine whether personal information was handled in accordance with the obligations contained within that Act. The process followed appeared to work well both for the entity that had been subject to investigation and for the individuals whose information had been impacted.

As a matter of policy, therefore, the AFC submits that the current legislative and self-regulatory framework would appear to adequately achieve the Government's objectives in considering this reform measure. In the absence of evidence-based justification for introduction of a mandatory breach notification obligation the Government should not pursue this outcome and we recommend that the Committee does not support passage of the Alerts Bill.

We submit consideration of additional compliance obligations to be introduced via the Alerts Bill amendments at this time is premature. In our view, the Government's focus is better placed to complete the framework to implement the currently enacted privacy reforms as a priority. In this regard we note a range of matters that have arisen as the industry endeavours to operationalise the amended laws and the potential need to refine some of the amended provisions or inclusion of additions to align the underlying policy with industry's processes. We accept that these will be taken up separately from the Committee process with the Government to be addressed in the lead up to the 12 March 2014 commencement.

Repayment History Information – s. 6V Definition

However, a particular matter that we submit that could be achieved by an amendment to reflect technical revision to better align the Government's policy with industry operations, relates to the definition of one of the new data-sets repayment history information (in s. 6V). Because it is a matter of technicality rather than a more substantive matter of policy, we submit that it could have bipartisan support to assist its enactment in the time available for this Parliament.

In summary, the Government's policy intention supported by industry was to facilitate the uniform disclosure by a credit provider / collection by a credit reporting body of repayment history information (ie on a monthly basis) given repayment cycles and dues dates for repayment vary for each individual depending on the type of consumer credit, the contractual obligations of the individual and the practices of the credit provider. However, in the s 6V definition the concept of month has been linked to the frequency of repayments rather than the frequency of reporting. By linking month to the repayment cycle rather than the reporting cycle in the s. 6V definition, the Government has been faced with the challenge of using the regulation-making power provided for in s. 6V to assist align repayment cycles (which as noted above may vary from contract to contract let alone individual to individual) to a monthly cycle by redefining concepts of whether a payment is a monthly payment or not, and the Code Drafters approved by the Privacy Commissioner developing an operational framework to complete the framework. While we remain fully supportive of this process given the need of the Code to be considered and registered by the Commissioner in time to facilitate implementation by the industry to meet the 12 March 2014 deadline, the underlying concern of the potential lack of clarity between the policy and the wording remains.

For this reason, should the Committee see fit to recommend passage of the Alerts Bill, the **AFC submits** that it may be appropriate for a further recommendation to be made

recognising industry's willingness to work with the Government to revise the s. 6V definition to facilitate introduction and enactment of a revised definition as part of the Senate debate process.

We would be happy to provide further information in support of the positions outlined above.

Kind regards.

Yours truly,

Ron Hardaker
Executive Director