AUSTRALIAN BANKERS' ASSOCIATION INC.
Strong banks – strong Australia

Level 3, 56 Pitt Street
Sydney NSW 2000
Australia
+61 2 8298 0417
@austbankers
bankers.asn.au

29 May 2017

Ms Kate Mills
Principal Adviser
ASIC Enforcement Review
The Treasury
Langton Crescent
PARKES ACT 2600
By email: Kate.Mills@treasury.gov.au

Dear Ms Mills

Self-reporting of contraventions by financial services and credit licensees

The Australian Bankers' Association (**ABA**) welcomes the opportunity to provide this submission to the ASIC Enforcement Review Taskforce's (**the Taskforce**) consultation paper on self-reporting of contraventions by financial services and credit licensees (**consultation paper**).

With the active participation of 25 member banks in Australia, the ABA provides analysis, advice and advocacy for the banking industry and contributes to the development of public policy on banking and other financial services. The ABA works with government, regulators and other stakeholders to improve public awareness and understanding of the industry's contribution to the economy and the community, to ensure Australia's banking customers continue to benefit from a stable, competitive and accessible banking industry.

Introductory comments

The ABA supports the ASIC Enforcement Review Taskforce's review of the current self-reporting regime for financial services and credit licensees (**breach reporting framework**).

The review of the breach reporting framework is an opportunity to address concerns regarding potential under reporting or delayed reporting of significant breaches. The review is also an opportunity to clarify self-reporting obligations and improve and standardise breach reporting practices across the financial services industry.

The ABA believes that any reforms to the breach reporting framework should:

- Ensure accountability and transparency of financial services and credit licensees
- Promote consumer protection
- Enable identification of emerging issues and risks, and
- Support ASIC to meet its law enforcement objectives.

The design of the reforms should take account of the findings and outcomes of ASIC's breach reporting surveillance project, which is looking at current industry breach reporting practices.

This submission sets out our response on the themes of the consultation paper, and provides responses to the consultation questions in **Attachment A**.

Strong banks – strong Australia

Improvements in conduct and culture

Better banking

The banking industry recognises that customers expect banks to keep working hard to make sure they have the right culture, the right practices and the right behaviours in place. The industry's Banking Reform Program is a multi-million-dollar investment by the industry, aiming to strengthen cultural and ethical standards, improve the offer of products and services and deliver better customer outcomes.

On 21 April 2016, the industry announced a comprehensive package of initiatives to protect consumer interests, increase transparency and accountability, and build trust and confidence in banks.[1]

The reform program was developed following close consultation with key stakeholders and regulators. It targets areas of concern to the community about governance, conduct and culture in banks. The six initiatives cover the areas of remuneration, complaints handling and dispute resolution, whistleblowing protections, reference checking and stopping misconduct moving around the industry, banking standards and regulation of banks.

The banks and the ABA continue to work closely with key stakeholders and regulators on implementation. Progress with the implementation of the reform program is being overseen by an independent governance expert[2], Mr Ian McPhee. Quarterly progress reports have been published by Mr McPhee since the announcement outlining implementation results, challenges and identifying areas requiring additional attention.[3]

Senior executive accountability

The ABA agrees with the Taskforce's sentiment that the breach reporting framework is not an appropriate mechanism for publicly naming individuals for accountability purposes. We believe that using the breach reporting framework to promote senior management accountability objectives is inconsistent with the primary objectives of breach reporting to enable the identification of emerging issues and risks, and support ASIC to meet its law enforcement objectives.

As part of the 2017 Federal Budget, the Government has announced substantial reforms to the governance of Authorised Deposit-taking Institutions to promote executive accountability. We support reforms to executive accountability requirements that can be demonstrated to support good governance, improve organisational competency, and drive accountability and transparency without triggering unintended consequences.

The ABA will be making submissions on the proposed banking executive accountability regime once consultation commences.

Principles based approach

The ABA supports clearly drafted, principles based legislation to effect any changes to the breach reporting framework. A principles based approach should allow flexibility to report breaches in a way that enables the identification of emerging issues and risks, and supports ASIC to meet its law enforcement objectives, without promoting a 'tick a box' approach, or triggering unintended outcomes, such as over reporting.

Similarly, ASIC regulatory guidance should be principles based. We do not support deeming of circumstances that are significant or should otherwise be reported as this approach may compromise the right risks and issues being reported to ASIC and reduce the breach reporting framework's focus on significance.

[1] http://www.bankers.asn.au/media/media-releases/media-release-2016/banks-act-to-strengthen-community-trust
[2] http://www.betterbanking.net.au/accountability/
[3] http://www.betterbanking.net.au/faster-industry-repair/ian-mcphee/

The ABA believes that reforms to the breach reporting framework should seek to minimise driving the over reporting of breaches that are not significant. A primary objective of the breach reporting framework is to enable the regulator to identify emerging issues and risks. Unnecessarily increasing volumes can add complexity to risk and trends analysis and trigger unintended consequences.

The significance test

The nature of the significance test has meant that there are different approaches to the application of the test to the circumstances of a breach, and differing expectations between industry and regulators on the nature of breaches that should reasonably be redefined. These differing expectations have contributed to concerns regarding potential under reporting or delayed reporting of significant breaches.

Objective test

The ABA agrees in principle with the Taskforce's position 1, that the significance test in section 912D of the Corporations Act should be retained but clarified to ensure that the significance of breaches is determined objectively. We suggest that there are a number of technical legal considerations in applying an objective approach, including whether the assessment should be made by a reasonable person in the same circumstances, similar to the business judgement rule.

The ABA also supports the development of additional regulatory guidance on the application of the objective test to be included in ASIC's *Regulatory Guide 78: Breach reporting by AFS licensees* [RG 78]. Consistent with the general approach to regulatory guidance, the guidance should be principles based to enable it to be applied in businesses of differing nature, scale and complexity and avoid unintended consequences. The development of the guidance should include extensive industry consultation to preserve the breach reporting framework's focus on significance, ensure the matters identified enable identification of emerging issues and risks, and manage operational impacts on industry and regulators.

The ABA does not support reporting suspected or potential breaches without applying the significance test. The ABA has been advised by banks that these proposed changes will drive increased volumes of breach reporting, at least in the first instance, while the new arrangements are being operationalised, or perpetually, where it is easier to operationalise reporting of all matters to avoid concerns about whether the test has been triggered or not. Where these breaches are not significant, reporting may affect the ability to identify risk trends and address key issues that impact customer outcomes. Reporting minor and technical breaches will also have resourcing impacts for both industry and regulators.

When the obligation to report arises

Uncertainty as to when the obligation to report arises has contributed to concerns regarding the delayed reporting of breaches.

The ABA believes the timely reporting of breaches is critical to enable identification of emerging issues and risks, and support ASIC to meet its law enforcement objectives.

Therefore, the ABA supports the Taskforce's position 3, breach to be reported within 10 business days from the time the obligation to report arises. We believe that the law already operates so the 10 day period arises from the date the Licensee becomes aware that the breach has occurred and establishes, applying the significance test, that it is significant. We do not believe that the 10 day period commences from the date the Licensee first becomes aware of the facts pertaining to the breach.

The relevant issue is whether from a policy perspective, it is adequate for the Licensee to report after establishing, applying the existing significance test, that a breach is significant.

The Taskforce has proposed a new standard to require the reporting of suspected or potential breaches without fully applying the significance test in order to bring forward reporting to ASIC. Instead the ABA suggests that the significance test could be amended to require Licensees to take account of information that reasonably evidences or gives reasonable grounds to suspect that a breach is

significant. This proposed approach would bring forward reporting to ASIC in circumstances where a long investigation is required to determine actual significance, while retaining the test's focus on significance.

Possible drafting changes could contemplate either the 10 business day timeframe commencing from when "the licensee becomes aware of the breach and has information that reasonably indicates that the breach, or likely breach, is significant", or "the licensee becomes aware of the breach and has reasonable grounds to suspect based on information known to the licensee that the breach or likely breach, is significant".

Working with ASIC

The ABA strongly supports a cooperative relationship between industry and the regulator.

ASIC operates a decentralised engagement model, meaning regulated entities liaise with multiple touch points across ASIC. It would be of benefit to consider opportunities for ASIC to work more holistically, especially with larger regulated entities. This may assist, for example, with encouraging better clarity and quality of breach reporting, with the provision of information that is more targeted to enabling ASIC to identify emerging issues and risks and meeting it law enforcement objectives. This may also assist identify efficiencies for ASIC and industry and avoid mixed approaches which can cause operational confusion. This proposed approach would give ASIC a better ability to prioritise and understand the relative significance of matters reported by Licensee.

The ABA also supports ASIC utilising existing processes and powers to identify and manage emerging risks and issues. We support ASIC undertaking market-wide surveillance programs into certain market and industry practices. The results of these reviews should be the subject of consultation with industry and stakeholders to identify any systemic issues. Where the reviews do not uncover systemic issues, these matters should continue to be addressed via targeted consultation and/or direct action between ASIC and the financial institution or regulated entity.

We also support ASIC's continued cooperation with the industry in relation to technical compliance issues and use of its relief powers to ensure the law operates as intended.

Good governance reporting

The ABA supports establishing a more formal framework for Licensees to choose to make good governance reports of activity or issues that are not significant breaches. This would improve transparency and accountability and promote a more cooperative approach between ASIC and industry.

The ABA has been advised by ASIC that good governance reports are received and managed through the enforcement teams. For good governance reporting to be successful, we suggest that a separate process be managed through the stakeholder teams.

Sanctions

The ABA strongly supports having appropriate sanctions for failure to report. We support the Taskforce's' positions 4 and 5 on increasing penalties for the failure to report, and introducing a civil penalty in addition to the criminal offence for failure to report.

The ABA does not support the introduction of an infringement notice regime. Infringement notice regimes are appropriate where there is a clear and easily established basis for a contravention. Even with the introduction of an objective test, an assessment of a contravention will need to be made in each case. We do not believe the infringement notice regime is fit for purpose for contraventions of the breach reporting framework. Introduction of an infringement notice regime is at odds with the co-operative approach between ASIC and industry contemplated at position 7.

Strong banks – strong Australia

Consumer credit regime

The ABA supports the Taskforce's position 9, to introduce a self-reporting regime for credit licensee's equivalent to the regime for AFS licensees under section 912D of the Corporations Act.

The ABA believes that a consistent approach to self-reporting of contraventions should be taken between financial services and credit licensees. However, there are differences between the designs of the two regulatory regimes that may require bespoke guidance to manage. For example, the financial services regime is more principles based than the consumer credit regime and particular guidance on the application of the significance test for technical breaches may be required to ensure a focus on requiring the reporting of significant breaches. We support either amendments to RG 78 to specifically cover credit licensees or new separate regulatory guidance.

We also believe that once a breach reporting regime is introduced, the scope of the Annual Compliance Certificate should be reduced to avoid duplication.

Reporting process

The ABA supports the Taskforce's position 8, to prescribe the required content of reports under section 912D and require them to be delivered electronically. We believe this would deliver immediate benefits by setting a common expectation on the content of breach reporting and drive improved data analytics for both industry and ASIC.

The design of the breach report content would need to be sufficiently flexible to allow Licensees to provide relevant information and avoid a 'tick a box' approach.

The ABA supports detailed consultation with industry on the design of the breach report content to ensure it elicits the most relevant information for the regulator, enables the identification of risks and issues and avoids unintended consequences.

Interaction with other frameworks

The ABA notes that changes to the AFS licensee and credit licensee breach reporting frameworks in isolation may require consequential amendments to other breach reporting frameworks, such as those under superannuation, banking and insurance laws. As part of the Taskforce's review, we suggest also considering harmonising the Licensee reporting obligations with Auditor reporting obligations, such as those under sections 311, 601HG and 990K of the Corporations Act, so that a consistent standard is applied.

Retroactivity

Any new requirements, or changes to the standard for breach reporting should apply prospectively. New breach reporting standards should not be required to apply retroactively, for example as part of compliance reviews and remediation programs.

If you would like to discuss any of the matters raised in this submission, please contact Christine Cupitt, Policy Director – Retail Policy (02) 8298 0416: ccupitt@bankers.asn.au.

Yours sincerely

Diane Tate
Executive Director – Retail Policy
(02) 8298 0410
dtate@bankers.asn.au

Attachment A: ABA response on consultation questions

Position 1: The significance test in section 912D of the Corporations Act should be retained but clarified to ensure that the significance of breaches is determined objectively

The ABA supports this position.

1.1 Would a requirement to report breaches that a reasonable person would regard as significant be an appropriate trigger for the breach reporting obligation?

The application of an objective standard is appropriate, however, the application of the objective standard should be against a reasonable person in the position of the Australian Financial Services Licensee (Licensee).

Any guidance on how to apply the test objectively should be principles based to avoid promoting a 'tick a box approach', or triggering unintended outcomes such as over reporting of minor or technical breaches. The development of the guidance should include extensive industry consultation to preserve the breach reporting framework's focus on significance, ensure the matters identified enable identification of emerging issues and risks, and manage operational impacts on industry and regulators.

1.2 Would such a test reduce ambiguity around the triggering of the obligation to report?

Perceived delays in reporting generally relate to establishing whether a breach is significant, rather than whether a breach has occurred. It is uncertain whether the application of an objective test will change the way that licensees assess the significance of breaches. We believe that Licensees will continue to apply professional judgement to apply the significance test in good faith. The change may however, provide a basis for a retrospective consideration of whether a breach should have been reported.

Position 2: The obligation for licensees to report should expressly include significant breaches or other significant misconduct by an employee or representative

The ABA supports this position in respect of representatives of the licence, such as financial advisers.[4]

2.1 What would be the implications of this extension of the obligation of licensees to report?

The ABA believes that this obligation would assist Licensees to report the conduct of representatives that would not otherwise constitute a significant breach. Reports should be limited to objective facts and not include subjective assessment such as whether a representative is suspected of not being of good fame and character. The obligation to report should be limited to relation to poor conduct and breaches related to the provision of financial or credit services as a representative of the licensee.

The obligation should be separate to s912D obligations, be accompanied by protections to promote procedural fairness, be linked to ASIC's role in overseeing and banning financial advisers and credit representatives where applicable, and work together with ASIC's current powers to request details of an individual who has allegedly engaged in breach behaviour.

We do not support an obligation to report on the conduct of employees who are not employed as representatives. We would be concerned by any change that involved publicly naming of individuals and continue to be mindful of both an individual's right to procedural fairness and risks in relation to defamation and employment laws.

[4] We note that some banks have expressed concern about the extended obligation applying to Australian Credit Representatives.

Position 3: Breach to be reported within 10 business days from the time the obligation to report arises

The ABA supports this position in principle.

3.1 Would the threshold for the obligation to report [outlined above] be appropriate?

As currently drafted, s912D does not clearly identify when a licensee's requirement to report is triggered. This ambiguity has resulted in differing expectations between ASIC and licensees. The ABA believes that the reporting threshold should change to clarify the expectation and address criticisms of delayed reporting. However we do not support the proposed change that effectively removes the application of the significance test from the trigger to report. The ABA does not support reporting suspected or potential breaches without applying the significance test as it will have resourcing impacts for both industry and regulators and where these breaches are not significant, may impact on the ability to identify risk trends and properly allocate resources.

The ABA believes that the law already operates so the 10 day period arises from the date the licensee becomes aware that the breach has occurred and establishes, applying the significance test, that it is significant. We do not believe that the 10 day period commences from the date the licensee first becomes aware of the facts pertaining to the breach.

The relevant issue is whether from a policy perspective, it is adequate for the Licensee to report after establishing, applying the existing significance test, that a breach is significant. The Taskforce has proposed a new standard to require the reporting of suspected or potential breaches without applying the significance test in order to bring forward reporting to ASIC. Instead the ABA suggests that the standard could be amended to require licensees to take account of information that reasonably evidences or gives reasonable grounds to suspect that a breach is significant. This proposal would bring forward reporting to ASIC in circumstances where a long investigation is required to determine actual significance, while retaining the test's focus on significance.

Possible drafting changes could contemplate either the 10 business day timeframe commencing from when "the licensee becomes aware of the breach and has information that reasonably indicates that the breach, or likely breach, is significant", or "the licensee becomes aware of the breach and has reasonable grounds to suspect based on information known to the licensee that the breach or likely breach, is significant".

3.2 Should the threshold extend to broader circumstances such as where a licensee "has information that reasonably suggests" a breach has or may have occurred, as in the United Kingdom?

Please see our response to 3.1.

3.3 Is 10 business days from the time the obligation to report arises an appropriate limit? Or should the period be shorter or longer than 10 days?

The 10 business days period is an appropriate period. A longer period, or more flexibility should be considered for reports under the new obligation covering individuals to allow time for legal and procedural fairness processes.

3.4 Would the adoption of such a regime have a cost impact, either positive or negative, for business?

During implementation, our members anticipate an increase in the volume of breaches reported while the new regime settles and the expectations of licensees and the regulator are understood. We anticipate a greater need for legal resources to properly apply the new regime.

Over time, it is unclear whether more significant breaches will be reported.

To manage costs, we support the standardised breach report content and electronic submission proposed in position 8.

Position 4: Increase penalties for failure to report as and when required

The ABA supports this position in principle.

4.1 What is the appropriate consequence for a failure to report breaches to ASIC?

The ABA supports a range of consequences for a failure to report breaches. These should include negotiated outcomes with ASIC, and enforcement outcomes, such as civil penalties.

4.2 Should a failure to report be a criminal offence? Are the current maximum prison term and monetary penalty sufficient deterrents?

Generally, we believe that a failure to report should be treated as a breach by the licensee entity. There should be very limited circumstances where an individual could be prosecuted for a breach of s912D and these should be limited to fraudulent, wilful and deliberately unconscionable acts.

Position 5: Introduce a civil penalty regime in addition to the criminal offence for failure to report as and when required

The ABA supports this position in principle.

4.3 Should a civil penalty regime be introduced?

The ABA supports the introduction of a civil penalty regime for failure to report. A civil penalty regime would need to consider whether the licensee intentionally failed to report a breach or whether it assessed the breach in good faith. Ambiguities relating to significance and timing would need to be rectified in order for a civil penalty regime to be appropriate.

Position 6: Introduce an infringement notice regime for failure to report breaches as and when required

The ABA does not support this position.

4.4 Should an infringement notice regime be introduced?

We do not support the introduction of an infringement notice regime. Infringement notice regimes are appropriate where there is a clear and easily established basis for a contravention and there is little room for subjective interpretation. Even with the introduction of an objective test, an assessment of a contravention will need to be made in each case. An infringement notice regime may drive over reporting, which has operational impacts for banks and the regulator.

Importantly, we do not believe the infringement notice regime is fit for purpose for contraventions of the breach reporting framework. An infringement notice regime is inconsistent with promoting accountability and transparency of financial services and credit licensees and enabling the identification of emerging issues and risks. This position is at odds with the proposed co-operative approach contemplated at position 7.

Position 7: Encourage a co-operative approach where licensees report breaches, suspected or potential breaches or employee or representative misconduct at the earliest opportunity

The ABA supports this position in principle.

4.5 Should the self-reporting regime include incentives such as that [outlined above]? What will be effective to achieve this? What will be the practical implications for ASIC and licensees?

The ABA strongly supports a cooperative relationship between industry and the regulator. In relation to breach reporting, we believe that cooperative approach should encourage better clarity and quality of breach reporting, with the provision of information that is more targeted to enabling ASIC to identify emerging issues and risks and meeting it law enforcement objectives. While we support our members

choosing to make good governance reports, we do not support an obligation to report suspected or potential breaches as such an obligation will unnecessarily increase reporting of minor and technical breaches, with operational impacts on industry and ASIC.

Incentives for self-reporting could properly include ASIC taking a more collaborative approach through the licensee's investigation and remediation processes and taking into account self-reporting in negotiated outcomes and enforcement actions.

ASIC operates a decentralised engagement model, meaning regulated entities liaise with multiple touch points across ASIC. It would be of benefit to consider opportunities for ASIC to work more holistically, especially with larger regulated entities. This may assist, for example, with encouraging better clarity and quality of breach reporting, with the provision of information that is more targeted to enabling ASIC to understand the relative significance of matters reported by licensee.

Position 8: Prescribe the required content of reports under section 912D and require them to be delivered electronically

The ABA supports this position.

5.1 Is there a need to prescribe the form in which AFS licensees report breaches to ASIC?

The ABA supports establishing a prescribed form for breach reporting. We believe this would deliver immediate benefits by setting a common expectation on the content of breach reporting and drive improved data analytics for both industry and ASIC.

A standard form would encourage more consistency and clarity across the industry on what needs to be reported, but the form must be flexible to serve financial services businesses of different size, nature and complexity, and allow information known at the time of the report to be reported with the facility to update as more information becomes available. This is particularly important where breaches are reported early. The form should allow for a licensee to provide a qualitative analysis of the breach and should not mandate reporting breaches under sections of the relevant act.

We note that there may be limited circumstances where a licensee may not use the form, or where only some parts of the form are completed, particularly where a breach is being reported early. Licensees would need certainty that not using the form, or not competing all sections of the form would not be a contravention of the breach reporting obligations.

We support use of an electronic portal to lodge notifications, but would like to preserve the ability to engage directly with enforcement and stakeholder teams.

5.2 What impact would this have on AFS licensees?

Many licensees have developed internal breach report templates and processes to streamline breach reporting activity. The benefit of a standard form would be the development of a cross industry common understanding of what should be reported.

Position 9: Introduce a self-reporting regime for credit licensees equivalent to the regime for AFS licensees under section 912D of the Corporations Act

The ABA supports this position.

6.1 Should the self-reporting regime for credit licensees and AFS licensees be aligned?

Yes, we support the introduction of a like breach reporting framework for credit licensees.

6.2 What will be the impact on industry?

The operational impacts on industry will be significant. Licensees will need to enhance their internal reporting processes, formalise breach and incident escalation processes and develop specific breach reporting capability. Industry should be given a sufficient transitional timeframe to implement any new regime.

Reporting processes should be harmonised for dual financial services and credit licensees. Once a breach reporting regime is introduced, the scope of the Annual Compliance Certificate should be reduced to avoid duplication.

Position 10: Ensure qualified privilege continues to apply to licensees reporting under section 912D

The ABA supports this position.

It is essential that qualified privilege continues to apply to licensees reporting under section 912D, to promote transparency and enable more detailed reporting.

7.1 Should the self-reporting regime for responsible entities be streamlined?

The ABA has not commented on this issue.

Position 11: Remove the additional reporting requirement for responsible entities

The ABA has not commented on this position.

Position 12: Require annual publication by ASIC of breach report data for licensees

The ABA supports this position in principle.[5]

8.1 What would be the implications for licensees of a requirement for ASIC to report breach data at the licensee level?

Consistent with the objective of ensuring accountability and transparency of financial services and credit licensees, the ABA supports reporting of breach data at licensee level. We believe the reporting framework should be carefully designed to manage risks that licensees take a more conservative approach to reporting, due to the risk of public scrutiny. The reporting should provide context around the raw data, provide insight that it is often the more prudent licensees who regularly report breaches and provide information on the rates of satisfactory remediation of breaches. The ABA does not support a public reporting framework being used to drive senior executive accountability, nor the naming of individuals.

8.2 Should ASIC reporting on breaches at a licensee level be subject to a threshold? If so, what should that threshold be?

If a change to the reporting trigger is introduced so that breaches that are not confirmed to be significant are r, only breaches that are subsequently confirmed to be significant should be published. The responsibility for assessing and confirming significance should remain with the licensee.

8.3 Should annual reports by ASIC on breaches include, in addition to the name of the licensee, the name of the relevant operational unit with the licensee's organisation? Or any other information?

Additional information to provide context to the raw breach data should be considered. This could include information on the percentage of breaches that resulted in enforcement outcomes.

The basis for publishing more information should focus on providing context and meeting the objectives of the breach reporting framework, rather than executive accountability purposes.

[5] We note that some banks have indicated they do not agree with the ABA's position and do not support the proposed public reporting.