Australian Banking Association

28 February 2020

Senior Adviser
Consumer and Competition Policy Division
Treasury
Langton Crescent, Parkes ACT 2600
By email: FSRCconsultations@treasury.gov.au

Dear Ms Keall

Recommendations 2.8, 2.9 and 7.2 - Strengthening breach reporting

At the release of the Final Report of the Royal Commission last year the banking industry committed to learning the lessons, fixing the problems and making things right.

One year on from the Royal Commission the banking industry has tougher rules imposed by the Government and regulators, a back to basics approach to banking which is squarely centred on the customer and a renewed focus on fixing culture.

The banking industry strongly supports the Government acting on the recommendations of the Royal Commission and is committed to working together to see 2.8, 2.9 and 7.2 of the Royal Commission are effectively implemented.

The ABA's position[1]

Effective regulation in the financial sector requires a strong, enforceable breach reporting framework, and in general the ABA supports the recommendations of the ASIC Enforcement Review Taskforce (ASICERT), as endorsed by the Royal Commission.

The new regime should be consistent with the recommendations of the ASICERT, be able to be practically and efficiently applied by industry and regulators, and ensure that the regulator has quality, timely access to information about breaches.

In our view, however, the regime outlined in the exposure drafts:

1. Is inconsistent in important respects with the recommendations of the ASICERT;
2. Is so complex that licensees, as well as regulators, will have difficulty in applying it in practice; and
3. Will capture such a broad range of reportable situations as to be counter-productive, diluting ASIC's source of intelligence on industry breaches.

We set out our observations in detail below.

Key points

- The subject of investigations under the breach reporting regime should encompass both the fact or otherwise of the occurrence of the breach *and* its significance.
- The requirement to report should not include circumstances where a licensee has, within 30 days after the reportable situation arose, investigated a breach and concluded either that the

[1] The ABA's response to recommendations 1.6 and 2.7 is outlined in a separate submission.

breach did not occur or, for circumstances where deemed significance does not apply, that the breach was not significant.

- The proposed section 912D should be revised and simplified, to make the implementation and operation of the new regime practical and efficient for both industry and regulators.
- The Bill should clearly define the circumstances in which a licensee is taken to have commenced an investigation for the purposes of the reportable situation provisions.
- Breaches of core obligations should be deemed significant where they result in material financial loss to clients having regard to the amount invested and the circumstances of the client/s in question (ASICERT). ASIC should be empowered to specify criteria for determining material loss using metrics based on amount of loss, number of clients affected, and other relevant matters. These criteria should be calibrated for different kinds of licensees.
- Breaches of civil penalty provisions should not be deemed significant per se (but are reportable if they are significant or otherwise deemed significant).
- If civil penalty provision breaches are deemed significant, civil penalties that attract pecuniary penalty maximums other than those specified in section 1317G of the Corporations Act or equivalent provisions in the ASIC or NCCP Acts should not be included.
- The exposure draft should be amended by removing the term ‘gross negligence’ and replacing it with more precise language that describes the kind of conduct intended to be caught.
- The obligation to report breaches by other financial services licensees should apply:
- where a licensee has reasonable grounds to suspect, rather than “there are reasonable grounds to suspect” that a breach has occurred, and
- only to reportable situations involving serious misconduct (as defined), or that give rise to material financial loss or damage to retail clients.
- For notification and remediation of clients following investigations, ASIC should have power to grant relief from the timing requirements where it thinks it appropriate, based on the circumstances and complexity of the breach. Further the time period for notifying clients should be extended to 21 days.
- The Bill should provide examples of how the transition provisions are intended to apply, to clarify under what regime various circumstances will fall depending on the time of occurrence of facts and the establishment of reasonable knowledge of them.

Yours sincerely

Jerome Davidson
Policy Director
Jerome.davidson@ausbanking.org.au

Australian Banking Association

About the ABA

The Australian Banking Association advocates for a strong, competitive and innovative banking industry that delivers excellent and equitable outcomes for customers.

We promote and encourage policies that improve banking services for all Australians, through advocacy, research, policy expertise and thought leadership.

Australian Banking Association

ABA submission - Strengthening breach reporting: Exposure draft legislation

1. Reportable situations

We note that the exposure draft introduces a concept of a 'reportable situation'. The way that this concept is cast immediately creates an inconsistency with the intention of the ASICERT. This is so in two respects – both of which are evident in this passage from the ASICERT Final Report:

> "The time for reporting would be extended from 10 to 30 days, but licensees should be required to make a report if they are investigating a breach and have not determined, within 30 days, whether it meets the significance threshold."

Two important considerations that this passage shows are:

- The ASICERT considered that the subject of 'investigations' in the context of its recommendations included an investigation into whether the breach was significant, in addition to the question of whether in fact the breach occurred.
- The obligation to report investigations was intended to apply where they had been underway for 30 days and *no conclusion had been reached* on either the existence of the breach and / or its significance.

The approach taken in the exposure draft is at odds with the above points because:

- The proposed new section 912D confines the concept of 'investigation' to the question of whether a breach occurred, relegating the question of the significance of the breach to a separate process of inquiry – to determine somehow (separately from investigating the breach) whether the relevant person 'reasonably knows' that the breach is significant under section 912DAA.
- The effect of the proposed new section 912DAB is that licensees must lodge a report as to the commencement of the investigation and its outcome, regardless of whether the investigation is concluded within 30 days and discloses no reasonable grounds to conclude that there has been a breach.

2. The subject of investigations

The removal of the question of significance from the concept of investigation in section 912D has some odd results. Under the draft, a 'reportable situation' does not arise in relation to an investigation unless a conclusion has been made that the breach in question is significant. Assuming the situation is one in which 'deemed significance' does not apply, then the licensee needs to assess significance having regard to:

a) the number or frequency of similar previous breaches;

b) the impact of the breach or likely breach on the financial services licensee's ability to provide financial services covered by the licence;

c) the extent to which the breach or likely breach indicates that the financial services licensee's arrangements to ensure compliance with those obligations are inadequate;

d) any other matters prescribed by regulations.

A proper assessment of all these factors is likely to take some time – even accounting for the use of term 'reasonably knows' and the definition of that term in 912DAA. Effectively, there's no time limit for this process of determining significance under the exposure draft. The 30-day time limit doesn't commence until a person reasonably knows that the breach being investigated is significant, so there would seem to be scope under this framework for lengthy inquiries to determine significance. A key

consideration driving the ASICERT recommendations was to eliminate the possibly that licensees could – legitimately or otherwise – take extended periods to determine significance.

ABA recommendation: The subject of investigations under the regime should encompass both the fact or otherwise of the occurrence of the breach *and* its significance.

The obligation to report

To reiterate the point made above, the intention of the ASICERT was to extend the period in which licensees could investigate and determine whether a breach was reportable, not to require that licensees report within that period regardless of the outcome:

> "the time frame should be extended so that licensees, in the first instance, have 30 days for conducting investigations and the initial assessment whether a matter is reportable."[2]

This is not the effect of the current exposure draft, under which the obligation to report arises immediately where there are reasonable grounds to suspect that a reportable situation exists (which includes the commencement of an investigation). The practical effect of this is that, for circumstances where the breach being investigated falls into a category of deemed significance, the obligation arises the moment the licensee turns their mind to whether the breach occurred, and is not extinguished if the investigation is concluded within 30 days and concludes that the breach didn't occur.

For situations where significance must be assessed by the licensee, the obligation arises if the licensee initially concludes, on the basis of the 'reasonable knowledge' provisions, that the breach is significant. However, if the licensee concludes, within 30 days, that the breach is not significant, the obligation to report is not extinguished. This is in addition to the point made above that the exposure draft allows the licensee to take an extended period to decide the question of significance before the 30-day time limit is triggered.

ABA recommendation: The requirement to report should not include circumstances where a licensee has, within 30 days after the reportable situation arose, investigated a breach and concluded either that the breach did not occur or, for circumstances where deemed significance does not apply, that the breach was not significant.

3. Complexity in determining obligations

3.1 Reasonable knowledge of the existence of reasonable grounds to believe

The obligation to report a situation to ASIC under the proposed regime arises where "there are reasonable grounds to believe that a reportable situation has arisen…"[3].

The situation must be lodged with ASIC "within 30 days after the financial services licensee first reasonably knows that there are reasonable grounds to believe the reportable situation".[4]

A financial services licensee must, then, having regard to the overall structure of the regime outlined above, ask itself whether it reasonably knows that there are reasonable grounds to believe that it:

- has breached a core obligation;
- is likely to breach a core obligation;
- has commenced an investigation into whether it has breached a core obligation;
- has committed gross negligence;

[2] ASIC Enforcement Review Taskforce Report, December 2017, p.9.
[3] s. 912DAB(1)
[4] S.912DAB(4)

- has committed serious fraud.[5]

To determine whether it reasonably knows that there are reasonable grounds to believe any of the above, the licensee, if it is not 'aware that the circumstance exists', will need to consider:

a) whether it is aware of a substantial risk that the circumstances exist; and

b) whether, having regard to the circumstances known to the person, it is unjustifiable to take the risk.

In addition, for circumstances outlined in 1 to 3 above, the licensee must ask itself whether it reasonably knows that there are reasonable grounds to believe that the breach in question is:

- significant; or
- in a category deemed to be significant.[6]

Added to the complexity outlined above is the fact that the timing of the 'reasonable knowledge' is critical. This is especially the case in relation to investigations of breaches. For example, if a licensee 'commences an investigation' (a concept we return to below), no reportable situation arises, and hence the time allowed for reporting does not commence, until the question of significance is determined. This depends on either:

1. The application of deemed significance (s.912D(5)); or
2. The application of the criteria outlined in section 912D(6).

Neither of these things will necessarily be clear at the time that the relevant compliance incident in first raised within a licensee. The licensee must continuously monitor for the point at which sufficient information is known to draw the conclusion that the breach is significant under one of the above heads. Presumably, at this point, the 30 days commences as that is when the licensee 'first reasonably knows that there are reasonable grounds to believe that the reportable situation has arisen'.[7]

Addressing the tests outlined above is likely to require heavy investment in resources for both large and small licensees.

ABA recommendation: The proposed section 912D should be revised and simplified, to make the implementation and operation of the new regime practical and efficient for both industry and regulators.

3.2 Commencement of investigation

A particularly problematic aspect of the regime is its operation in relation to commencement of investigations. The problem is made more acute by the inconsistency with the intent of the ASICERT as outlined above – i.e. that no obligation to report should arise where an investigation completed within 30 days determines that no breach occurred or that a breach is not significant.

As the draft stands, the critical problem is in determining the point at which an investigation commences. On a plain reading of Bill (assuming the significance test is satisfied), the 30-day time period will commence when a licensee reasonably knows that there are reasonable grounds to believe that it has commenced an investigation. This is too vague a concept for industry, regulators, and ultimately courts, to apply. For example:

- does an external audit or internal audit (with findings of potential breaches) trigger the start of an investigation?
- proactive thematic work looking into area of suspected weak compliance?
- commencement of legal advice to assess whether there has been a breach or likely breach?

[5] s. 912D(1)&(2)
[6] s.912D(1)(b)
[7] S.912D

- branch staff looking into a customer's file to substantiate a complaint.

The Bill should be clearer on the point at which a licensee is taken to have commenced an investigation.

In the absence of a definition, licensees (and others) will be left to determine on vague criteria whether they should regard an investigation to have commenced. To manage compliance, it is likely that licensees will substantially over report potential breach incidents, diluting the quality of intelligence on breaches received by ASIC.

ABA recommendation: The Bill should clearly define the circumstances in which a licensee is taken to have commenced an investigation for the purposes of the reportable situation provisions.

4. Deemed significance of breaches

We note that the circumstances in which the exposure draft deems a breach to be significant (section 912D(5)) are largely consistent with the recommendations of the ASICERT. However, in our view, the practical effect of two of the deeming provisions is such that a very large portion of potential breach incidents, regardless of their actual significance, will be require a report to be lodged with ASIC, with the result that the quality of intelligence going to ASIC will be diluted and the intent behind having a significance threshold will be undermined. The two provisions in question are s. 912D(5)(b)&(c):

> (b) the breach constitutes a contravention of a civil penalty provision; or
>
> (c) the breach results, or is likely to result, in loss or damage to clients or, in the case of a managed investment scheme, members of the scheme.

The problem arises because neither provision has a materiality or significance threshold. Notably, the absence of a materiality element in relation to the deemed significance of 'loss or damage' to clients, is inconsistent with the recommendation of the ASICERT.

4.1 Materiality of loss

The ASICERT specifically contemplated a materiality element, including in its list of matters that should be deemed significant:

> "Breaches that result in or have the potential to result in *material loss to clients having regard to the amount invested and the circumstances of the client/s in question*"[8] [emphasis added]

The ASICERT came to this conclusion aware of the fact that under the existing regime, losses that were substantial from the individual client's perspective could nevertheless be discounted as insignificant by the licensee, relying on the overall context and size of the business etc. The ASICERT's conclusion balances addressing that concern while retaining a sensible materiality threshold for determining significance where there has been loss to clients.

Abandoning any materiality element for this purpose – as the exposure draft proposes to do – results in the potential for multiple reporting of breaches that would by any objective standard be regarded as insignificant. For example, any loss as a result of a breach – 5 cents, 50 cents, $1 – even where these are isolated and / or have quickly been identified and remediated, would give rise to a reporting obligation. That result would drive up compliance costs for industry without any apparent benefit from a regulatory perspective.

Additionally, the term 'loss or damage' could be interpreted to extend to non-financial loss – something that is very difficult for licensees to ascertain or quantify. The term should be confined to (material) financial loss.

ABA recommendation: Breaches of core obligations should be deemed significant where they result in material financial loss to clients having regard to the amount invested and the circumstances of the client/s in question (ASICERT). ASIC should be empowered to specify

[8] ASIC Enforcement Review Taskforce Report, December 2017, p.6

criteria for determining material loss using metrics based on amount of loss, number of clients affected, and other relevant matters. These criteria should be calibrated for different kinds of licensees.

4.2 Breaches of civil penalty provisions

While the deeming of breaches of civil penalty provisions as significant is consistent with the ASICERT, the wide range of contraventions that now attract civil penalties means that in practice, this deeming provision will capture a high percentage of incidents that come to light through licensees' compliance systems.

A large number such incidents are likely to prove to be insignificant and reporting them to ASIC will needlessly increase the volume of reports that the regulator has to triage. In our view, this is a rare instance in which the ASICERT recommendations should be departed from. Breaches of civil penalty provisions should not be deemed significant per se but should instead be subject to the tests applicable to breaches generally – i.e. are reportable if they are significant or deemed significant under other provisions.

ABA recommendation: Breaches of civil penalty provisions should not be deemed significant per se (but are reportable if they are significant or otherwise deemed significant).

4.3 Lower level civil penalty regimes

While most civil penalty regimes in and corporate and financial sector legislation will have the penalties set out in section 1317G of the Corporations Act or its equivalents, there remain some regimes with much lower penalties. For example, the regime for enforceable code provisions that is being consulted on in parallel with this Bill, proposes a civil penalty for breaches of such provisions that would have a maximum of 300 penalty units. Requiring any such breach to be reported, regardless of significance, would mean that numerous insignificant code breaches would be required to be reported to ASIC.

It can be presumed that, given the much lower penalty cap, this kind of contravention was not considered by the legislature to be of the same order of significance as breaches of general civil penalty provisions that attract the penalties in section 1317G. For that reason, they should not be deemed to be significant under this regime.

ABA recommendation: If civil penalty provision breaches are deemed significant, civil penalties that attract pecuniary penalty maximums other than those specified in section 1317G of the Corporations Act or equivalent provisions in the ASIC or NCCP Acts should not be included.

5. Reporting gross negligence and serious fraud

Section 912D(2) introduces two new concepts as reportable situations. These are where:

> (a) in the course of providing a financial service a licensee or representative has engaged in "conduct constituting gross negligence", or
>
> (b) the licensee or representative has committed "serious fraud".

These proposals are additional to those suggested by the ASICERT. In the form set out in the exposure draft, it will be difficult for licensees to determine whether 'gross negligence' or 'serious fraud' has been committed. Such questions are usually determined by the courts according to settled legal principles or criminal statutes with the benefit of a trial.

In addition, the way that s.912D(2) is framed implies that the concepts it refers to are well defined. While this may be somewhat true of 'serious fraud' is recognisable, the same cannot be said of the term 'conduct constituting gross negligence'.

Given the serious consequences – civil and criminal – attaching the non-compliance with this regime, concepts should be at least reasonably ascertainable by licensees. Use of the term 'gross negligence'

alone is not sufficiently precise. Rather than use the term 'gross negligence', the Bill should specify with greater precision the kind of conduct that it intends to capture.

ABA recommendation: The exposure draft should be amended by removing the term 'gross negligence' and replacing it with more precise language that describes the kind of conduct intended to be caught.

6. Reportable situations in relation to other financial services licensees

We support the addition of this reportable situation but in our view it should be modified. The test should be whether the licensee itself has reasonable grounds to suspect and any investigation into whether a licensee has breached this provision by not reporting another licensee's breach should be focused on what the licensee itself reasonably suspected at the time rather than an objective assessment of whether it should have suspected a reportable situation had arisen in relation to another licensee.

This is an offence provision and is extremely onerous. It is unreasonable to subject licensees to this obligation to report the wrongdoing of others on the basis of a mere suspicion without applying some level of seriousness to the types of reportable breaches. Otherwise, this obligation may trigger reporting obligations on licensees to report even very minor reportable situations of other licensees, failing which it will commit an offence.

Additionally, it is difficult for a licensee to determine that a reportable situation has arisen about another licensee owing to limited or no access to the relevant information.

Finally, the obligation to report suspected reportable situations relating to other licensees could lead to cross-reporting of entities within a corporate group where there is more than one licensee within the group. The ED should include an exemption from reporting under s.912DAC where members of the same corporate group would be required to report on one another (i.e. a single report from the licensee engaging in the breach is sufficient).

ABA recommendation: The obligation to report breaches by other financial services licensees should apply:

- **where a licensee *has* reasonable grounds to suspect, rather than "there are reasonable grounds to suspect" that a breach has occurred, and**
- **only to reportable situations involving serious misconduct, or that give rise to foreseeable material financial loss or damage to retail clients.**

7. Notifying and remediating clients

We support the new provisions in Subdivision C but in our view they could be improved by making some additions. Firstly, the regime should factor in large scale remediation projects. In such circumstances:

- ASIC should be given the power to grant relief from complying with the timing requirements under this subdivision based on the circumstances and complexity of the breach and where it has agreed with the licensee on a remediation plan.
- licensees should be given the discretion to hold off from paying a client provided the licensee compensates the client for delayed payment if that client is part of a broader ongoing investigation and ASIC has agreed to it.

It may not be reasonable to notify a client within 10 days and pay a client within 30 days if that client is part of a larger scale remediation project. Indeed, for notifications, even for projects of a lesser scale, 10 days is a short period to obtain all internal approvals for member communications – at least 21 days would be preferable, but should be subject to ASIC's discretion as outlined above.

Secondly, for remediation, 30 days to pay after an investigation is completed may be inadequate in circumstances other than those outlined above. For example, in superannuation, the amount may not be able to be so quickly ascertained, for instance, where the compensation would involve unwinding the clients' tax position which would require consultation with the ATO.

ABA recommendation: For notification and remediation of clients following investigations, ASIC should have power to grant relief from the timing requirements where it thinks it appropriate, based on the circumstances and complexity of the breach.

8. Transition date 1 April 2021

The transition regime in the draft Bill is unclear in some respects. For example, the intention appears to be that the existing regime continues to apply to breaches which occurred prior to April 2021 (clause1670A(2)). However, clause 1670B provides that the reporting obligations in proposed sections 912DAB "apply in relation to reportable situations arising on or after 1 April 2021". It is conceivable that the facts giving rise to a reportable situation could occur prior to 1 April 2021, but that the 'reportable situation' arises after that date. This is because reportable situations arise not necessarily when things occur but when parties have certain states of knowledge of them.

The draft legislation proposes significant changes to the existing breach reporting regime. This will no doubt trigger substantial changes to licensee' systems and processes, which staff will then need to be trained on. Under the proposed timetable, there is only nine months from the date of royal assent to when the new regime commences. This is a very short window to achieve an orderly transition, especially for licensees with diverse or complex business structures. Consideration should be given to deferring the transition date to 1 January 2022.

In the interim, evidence from ASIC suggests that industry breach reporting practices improved measurably after the Royal Commission, evidenced by a significant increase in the number of breaches reported.

ABA recommendation: The Bill should provide examples of how the transition provisions are intended to apply, to clarify under what regime various circumstances will fall depending on the time of occurrence of facts and the establishment of reasonable knowledge of them.

ABA recommendation: The transition date should be 1 January 2022.