

Niki De Mel
Strategic Policy Adviser
Strategy Group
Email: BR.submissions@asic.gov.au

Dear Ms De Mel,

Thank you for the opportunity to provide feedback to Consultation Paper 340, specifically in relation to the Draft Regulatory Guide 78 and the proposals outlined in the Consultation Paper.

Bendigo and Adelaide Bank Limited (“**the Bank**”) supports the intent behind the significant breach reporting regime as it is paramount for industry participants to be provided with greater certainty on breach reporting obligations and also for ASIC to receive reports in a timely and consistent manner. However, the Bank has a general concern as to whether these outcomes will be effectively achieved, given the breadth of the new reporting obligations.

Multiple stakeholder sessions and meetings with industry bodies have not brought us any closer to understanding with greater certainty and clarity the exact scope of the new reforms. Repeat training sessions for first-line risk and compliance staff are also expected to run on an ongoing basis (pre and post October 2021) to equip risk and compliance staff with the requisite skills to assess whether an event is a reportable situation. Second-line staff will perform the final assessment as to whether an event is a reportable situation.

To achieve the objective of the reforms, we believe there needs to be detailed and focused guidance to help licensees understand when a reportable situation arises. Under the ‘deemed significance’ test, the high volume of provisions that could currently appear to require reporting, seems to detract from the original intent of strengthening and clarifying the existing breach reporting requirements and allowing ASIC to detect significant non-compliance early. The Bank is concerned that the resources and manual effort required to ensure compliance with the reforms may in fact impede timely management of events.

The feedback listed below has been referenced to the specific proposals outlined in the Consultation Paper and should be read as such.

B Breach reporting by AFS licensees and credit licensees

B1 We propose to give consistent guidance for AFS licensees and credit licensees on how they can comply with the breach reporting obligation, with examples of how the obligation applies in particular situations.

B1Q1 – The Bank would welcome any further detailed guidance from ASIC given the challenges present in the new reforms. The Bank does not have further comments with respect to specific guidance on the structure and operation of credit licensees.

B2 We propose to include case studies and scenarios to supplement our general guidance and help illustrate key principles as they might apply to different licensees, industries and business models.

B2Q1 – Guidance should be clearly set out for scenarios where compliance breaches go undetected for a period of time. In assessing the extent of the compliance arrangements being inadequate, one of the factors outlined in 78.42: Table 3 is to ask questions such as the length of time the incident went undetected. We would appreciate more clarity on the term ‘undetected’ given that there could be scenarios where an event is at first instance, not considered a compliance breach based on sound legal interpretations and advice and then later assessed as a breach due to introduction of new factors and systems. We suggest the length of time that has passed between receiving the first legal advice and then

re-evaluating the incident based on new factors should not of itself be considered as the breach having gone undetected for a period of time or that compliance arrangements have been inadequate.

B3 Draft RG 78 identifies where the existing breach reporting obligation (as in force immediately before 1 October 2021) continues to apply to AFS licensees: see draft RG 78.14–RG 78.18.

The Bank has no further comments with respect to this proposal.

The Bank notes that at paragraph 78.28 of the draft Regulatory Guide 78, subparagraphs (a) to (e) are listed. The Bank has noted that sub-paragraph (c) is not included, and queries if this is a typographical error.

B4 We propose to provide high-level guidance to help AFS licensees and credit licensees identify what they must report to ASIC, including guidance on: (a) what is a ‘reportable situation’ (see draft RG 78.19–RG 78.25); (b) whether a breach or likely breach of a core obligation is significant (see draft RG 78.26–RG78.45); (c) when an investigation is a reportable situation (see draft RG 78.46–RG 78.57); (d) what are ‘additional reportable situations’ (see draft RG 78.58–RG 78.60); and (e) what are reportable situations about other licensees (see draft RG 78.61–RG 78.67).

B4Q1 – The Bank agrees with ASIC’s proposed approach and would welcome further guidance to increase clarity on what becomes reportable to ASIC and when it becomes reportable.

B4Q3 – Guidance on this aspect would be appreciated. Based on the new reforms, under the Financial Sector Reform Act 2020, it is the Bank’s understanding that a breach or a likely breach of a core obligation becomes significant where the incident is one of the following:

- a) *a commission of an offence under any law and the commission of the offence is punishable on conviction by a penalty that may include imprisonment for a maximum period of 3 months or more (for dishonesty) or 12 months or more for any other cases;*
- b) *a contravention of a civil penalty provision under any law;*
- c) *a contravention of subsection 1041H(1) of the Corporations Act 2001 or subsection 12DA(1) of the ASIC Act (misleading or deceptive conduct in relation to a financial product or a financial service);*
- d) *results, or is likely to result, in material loss or damage to members or customers; or*
- e) *a commission of gross negligence or serious fraud.*

The Bank would welcome guidance on how the above provisions tie in with the relevance of a core obligation being significant. Our original interpretation of the law under the objective test (deemed significance) was to first consider whether an event is a breach or a likely breach of a ‘core obligation’ and then assess whether the event is significant. This meant limiting our focus to Sections 912A and 912B of the Corporations Act 2001 and Section 47(1) of the National Credit and Consumer Protection Act 2009. For instance, assessing a contravention of a civil penalty provision or a key requirement under the National Credit Code as significant and therefore reportable, has no relevance to the definition of a core obligation. Given this uncertainty, in an event of a breach of financial services law, it is not clear whether AFS licensees are also expected to assess that breach against one of the core obligations stipulated under the Corporations Act 2001 or the National Credit and Consumer Protection Act 2009.

Timeline of when an investigation starts

B4Q4 – The Bank would welcome further guidance on when an investigation becomes a reportable situation. It is hard to ascertain from the examples provided in the draft regulatory guide when the timeline for investigation commences. The regulatory guide indicates that some level of information gathering that amounts to a searching inquiry or human effort applied to ascertain facts are examples of when investigation has commenced. However, RG78.49(a) indicates that merely entering a suspected compliance issue into a risk management system is unlikely to amount to a searching inquiry. This appears to be a quandary - in many instances, entering the risk event into the risk management system has occurred because an investigation has already commenced to determine whether there is a compliance issue. The inquiry into the issue continues after the event has been logged into the system. We submit that specific examples of when the chronology of an investigation starts and does not start should be expressly included in the regulatory guide.

Material loss and damage

B4Q5 – Yes, we would appreciate further guidance on what constitutes ‘material loss or damage’. Currently, there is no threshold for materiality. The primary challenge we face is in quantifying material loss or damage. For example, should losses simply be quantified at the amount which should be paid to the customer to put them back into the same position had the wrongful act not occurred? In the event of physical loss, destruction or damage, a financial calculus may be possible, however, this becomes particularly complex when assessing loss/damage on an emotional and mental scale rather than with financial metrics. Would the customer need a legally enforceable right to damages or prove their losses on the balance of probabilities before being assessed for material loss or damage? Particularly, guidance on how a bank can best translate the different vulnerabilities experienced by a customer to quantify material loss or damage would be valuable. Vulnerable customers are usually more at risk of harm or loss due to their personal circumstances; however, this does not become apparent until after an event has occurred.

Meaning of ‘serious fraud’ and ‘gross negligence’

B4Q6 – Further guidance on what constitutes ‘serious fraud’ and ‘gross negligence’ would be helpful. Key challenges include differentiating between mere ‘negligence’ and ‘gross negligence’ and ‘fraud’ and ‘serious fraud’. We understand that gross negligence is meant to cover something more than ordinary negligence, however in the absence of a legal definition, it is unclear what types of situations would constitute more than a failure to exercise the standard of care or prudence that would ordinarily constitute mere negligence, or how to assess the materiality of the damage that results from the event, to then term the event an act of gross negligence. There are similar challenges with also assessing the difference between ‘fraud’ and ‘serious fraud’. Generally, fraud is the use of deceit to obtain another person’s property. Is seriousness then to be defined based on the amount of financial loss, sophistication in executing the offence, and who the offence was by committed by (professionals etc)? Given these uncertainties, we suggest that express examples of acts of gross negligence and serious fraud should be included in the regulatory guide.

Reportable Situations About other Licensees

B4Q7 – Further guidance on reportable situations about other licensees would be appreciated. Specifically, the Bank seeks clarification on the ‘trigger point’ of reporting to ASIC. For instance, if the matter has come to light through a detective control (such as a customer complaint) that suggests that a Broker may require further investigation, when should ASIC be notified? It is also not clear what or when BEN (as the credit provider) must inform the Aggregator when a reportable situation arises. And, in terms of timeframes, is there an obligation to notify the Aggregator before, at the same time as notifying ASIC, or post-report?

In addition, effective 1 October 2021, a credit provider will be sharing Combined Industry Forum metrics to Aggregators which will then give them greater abilities to monitor Broker conduct across the industry. However, this raises some questions from an enterprise perspective. If a credit provider provides this data to the Aggregator and that data on its own has not triggered a credit provider to investigate the Broker but the Aggregator (when they collectively look at all the data they receive across all banks about that Broker) commence an investigation, does the Aggregator have an obligation to inform the credit provider that they have commenced an investigation that is reportable to ASIC? Clarity on this issue would be helpful.

Alternatively, if the credit provider provides this data to the Aggregator and that data has triggered the credit provider to investigate that Broker further and report to ASIC, what is the credit provider’s obligation to notify the Aggregator that it has triggered reasonable grounds for reporting to ASIC?

B5 We propose to include guidance in draft RG 78 about the obligation for licensees to report to ASIC within 30 days after they first know that, or are reckless with respect to whether, there are reasonable grounds to believe a reportable situation has arisen: see draft RG 78.68– RG 78.81.

B5Q1 – Yes, we would appreciate further guidance to help licensees understand when to report to ASIC. Specific guidance is requested in the next question.

B5Q2 – We seek further guidance on what may amount to ‘knowledge’, ‘recklessness’ and ‘reasonable grounds’. In assessing ‘knowledge’ or when the licensee ‘first knows’, does ASIC consider that ‘knowledge’ stems from the employee who has the requisite expertise and responsibility to assess whether a reportable situation has arisen? Similarly, with ‘recklessness’, more guidance is desirable to assess what a ‘substantial risk’ means and how the test of substantiality is to be applied in the circumstances.

Further, the meaning of ‘reasonable grounds’ lends itself to the specific context in which it is used depending on the circumstances. For reasonable grounds to exist, it is expected that reliable information and facts are evident for a reasonable, prudent person to rely on before inferring that a reportable situation has arisen. We suggest that further examples that apply these terms be included in the regulatory guide, particularly as to how they relate to an assessment of deemed significance under Section 912D(1)(a) of the Corporations Act 2001.

B6 We propose to provide general guidance on the types of information we will include in the prescribed form that licensees must use to provide reports to ASIC: see Table 8 in draft RG 78.

B6Q1 – Q3: We do not require further guidance on the questions in the prescribed form, however, we do have concerns with the time it will take to respond to those questions and upload each significant breach to the portal. It is our understanding that a bulk upload option will not be available when the new reforms take effect 1 October 2021. In such an instance, we have to manually upload each significant breach into the portal. Given the expected rise in the number of significant breaches and taking into account the time required to manually upload each breach, we have concerns around how this cumbersome process may impact on staff productivity. We also request further clarification as to whether the questions on the proposed prescribed form are to be completed in addition to the 60+ questions on the portal currently. Further guidance on this is needed to ensure that we have adequate resources in place to manage the breach reporting process.

B7 We propose to provide high-level guidance on compliance systems for breach reporting to help licensees comply with the breach reporting obligation: see Section D of draft RG 78.

B7Q1 – B7Q3: We welcome high-level guidance on compliance systems for breach reporting, however it may not be possible to apply a blanket approach to all facets of our compliance systems. For instance, a significant uplift to the user interface of our risk management system is required to ensure that all variants of reportable situations are captured in the system for effective event management. It is expected that this uplift will allow for the information within the system to be extracted and fed into the ASIC portal without time constraints. This is a significant piece of work for select operational risk management staff, in addition to business-as-usual activities. We are unable to provide specific feedback on this question until we can assess the kind of guidance ASIC is expecting to provide and how it will apply specifically to our compliance systems and what cost pressures are involved.

We have not provided any feedback on proposals C1 and C2 as the Bank does not provide personal advice regarding relevant financial products and does not employ any mortgage brokers.

Thank you once again for the opportunity to provide feedback. We look forward to further opportunities to contribute to this important regime. If you wish to discuss further, please do not hesitate to contact Kate Haigh on [REDACTED] or via email [REDACTED]

Kind regards,

John Price
Head of Group Regulatory Compliance
Bendigo and Adelaide Bank Limited