Australian Banking Association

03 June 2021

Niki de Mel
Strategic Policy Adviser, Strategy Group
Australian Securities and Investments Commission
By email: BR.submissions@asic.gov.au

Dear Ms de Mel

Consultation Paper 340: Breach reporting and related obligations

The Australian Banking Association (**ABA**) welcomes the opportunity to comment on the consultation released by the Australian Securities and Investments Corporation (**ASIC**) regarding the breach reporting and related obligations due to come into effect on 1 October 2021.

Our position

The reforms to the breach reporting framework following the Financial Services Royal Commission (and the ASIC Enforcement Review Taskforce Report) are the most significant changes to the regime since its inception. It is vital that policymakers and regulators implement the regime prudently, if it is to be effective in achieving its aims, and viable from the perspective of implementation by the sector.

The ABA has participated in each step of the implementation process for these reforms and remains an active and interested participant. We await the completion of the final regulations by Government, which are an important component of the regime and vital to its viability. These regulations will be of significant relevance to the final ASIC Regulatory Guide (the Guide).

Key recommendations

Given the complexity of the regime, there are a number of matters which should be addressed or further explained in the Guide. We set these matters out below.

Avoiding duplication

There are various circumstances where the obligation to report a matter may technically fall on more than one entity. For example, where one licensed entity is a related party of another. There may also be reportable situations that involve a number of different representatives who have committed distinct but related breaches. The regulatory Guide should make clear that, once a matter is reported, any other obligation to report in respect of the same matter is extinguished.

Clarity over legal definitions

The Guidance would benefit from further clarity regarding the types of situations that comprise reportable instances. For example, more examples and guidance are sought with regard to:

- the circumstances that ASIC considers constitute ‘recklessness’ and “reasonable grounds”; and
- where ‘gross negligence’ should be taken to be present.

The scope of an investigation

The Guide should make clear that:

simple fact finding and assessment processes in response to complaints or internally identified incidents do not, of themselves, constitute the commencement of an investigation under the Act.

- an investigation is *complete* once it is decided whether a reportable situation has occurred, and does not, for instance, require conclusions as to the quantum of consumer loss or numbers of customers impacted by the breach, to be regarded as complete.

Treatment of criminal offences

The Guide should confirm that:

- breach reports made by reason of the provisions relating to 'serious fraud' or deemed significant criminal offence provisions will be taken only as indicating the presence of reasonable grounds to believe that offences have been committed and not as an admission that an offence has been committed, for the purpose of any other proceedings.
- if the licensee is satisfied that the necessary mental fault element for any "serious fraud" or deemed significant criminal offence is not present, there is no reporting obligation just because the physical elements of the fraud or offence are present.

Examples of breaches of deemed significance

If the regulations exclude the licensing obligation provisions (in the Corporations Act and Credit Act) from breaches of deemed significance, they will nevertheless remain 'core obligations' under the new regime and it would be useful if ASIC provided additional examples of what circumstances would constitute a significant breach of these provisions.

In addition, further examples on the kind of circumstances that ASIC considers constitute 'material loss' for the purposes of assessing significance, would be useful, as would high-level guidance on what constitutes material 'non-financial loss'.

Reporting of multiple breaches related to a single cause or systemic issue

It would be helpful for ASIC to provide further guidance on:

- breaches with multiple related scenarios or instances; and
- expectations relating to updates to previously reported matters.

In addition, the Guide should acknowledge the role of aggregators in facilitating the provision of credit to clients, and to set out its expectations in situations where:

- an aggregator is unhelpful in addressing broker misconduct[1]; and
- an aggregator is not a licensee for the broker and the breach report is to be provided to the broker, but the broker is not appropriately addressing the conduct concerned.

Regulatory portal

We note that ASIC's regulatory portal will play a key role in the operationalisation of the new breach reporting regime. We note that we have raised concerns with ASIC about the functionality of the portal, especially the absence of a capability to accept batch reporting of breaches. We would welcome further engagement with ASIC on the operational aspects of the portal prior to the new regime taking effect in October.

Some additional observations on how the portal could be improved are set out in the Appendix.

[1] Where the broker is a credit representative of the Aggregator.

Australian Banking Association

Other comments

We submit that ASIC's guidance on the new notification, investigation and remediation of breaches obligations should be incorporated into RG 256.

The draft Guide is heavily focussed on the obligations arising under the Corporations Act. In our view, more commentary/guidance/examples are needed in respect of the obligations of credit licensees under the National Consumer Credit Protection Act (Credit Act).

ASIC should also consider any implications the new regime could have on the protection of whistleblowers. In particular, it could provide guidance on how licensees should ensure that reporting of breaches of the whistleblower provisions (or investigations of these beyond 30 days duration) does not increase the risk of inadvertent disclosure of the identity of the whistleblower.

More detailed comments on each of these items are summarised in the Appendix.

We would welcome further engagement in relation to these matters as the start date for the new regime approaches. Should you require any further information in relation to the points made above, please do not hesitate to contact us.

Yours sincerely

Jerome Davidson

Director, Legal Affairs

[redacted]

Australian Banking Association

Appendix: Detailed feedback

1. Reportable situations

1.1 Recklessness and reasonable grounds

1.1.1 'Recklessness'

Example 7 in the draft guide provides an obvious example of what would constitute recklessness. It would be helpful for ASIC to include a more nuanced case study or example where recklessness might arise. For example it would be helpful for ASIC to clarify that a licensee would not be reckless in the following circumstances:

- where there are partially known facts (this could arise eg. where a licensee receives a complaint or is aware of rumours but does not have enough detail to fully investigate the potential breach and are unable to get more information from the complainant), or
- where the facts that the licensee is aware of would not give rise to a reportable situation (but there is in fact, a reportable situation, and the licensee has failed to report on the basis of a good faith belief in the original facts provided). This could arise, for example, where an event is raised with wrong information and so, mistakenly, the issue is not identified as reportable.

1.1.2 'Reasonable grounds'

Further, it would be helpful for ASIC to include additional guidance on when licensees should conclude that "reasonable grounds to believe" a reportable situation exists has arisen. Some case studies on factual circumstances which would, in ASIC's view, give rise to reasonable grounds to believe (and those which do not) would be useful.

In particular it would be helpful for ASIC to confirm that the breach reporting obligations, and the general licensee conduct obligations including to act honestly, efficiently and fairly, do not combine to create a duty for a licensee to proactively monitor representatives or other licensees for:

i. conduct of that other licensee, or representative on behalf of other licensees, that may constitute breaches of financial services laws or consumer credit laws; or

ii. private conduct of that other licensee or representative that may constitute serious fraud, or a breach of financial services laws or consumer credit laws entirely unrelated to the first licensee.

1.2 'Gross negligence'

The term "gross negligence" is not defined in the Corporations Act or in the Explanatory Memorandum. The concept of gross negligence is more developed and understood in other jurisdictions such as the United States. The courts in Australia have not given clear guidance as to what this concept means.

Guidance from ASIC in the new RG 78 as to the meaning of "gross negligence" would be useful so that all licensees and representatives of licensees are able to assess their conduct against this standard. For example, does ASIC essentially regard "gross negligence" as carelessness to an extreme degree? Some of the challenges in identifying gross negligence include:

- Whether grossly negligent conduct by the licensee or its representative is reportable in the absence of negative effect on customers or clients.
- When conduct by representatives should be attributed to the licensee or undertaken as a representative of the licensee for the purpose of s 912D(2) (given that the portal wireframe requires the licensee to indicate whether the report relates to its conduct, a representative's conduct, or both).

1.3 Investigations

1.3.1 Time of commencement RG78.51

The time of commencement of investigations is important in determining reporting obligations under the regime. One key point requiring clarification is that , for the purposes of reporting of investigations, commencement is not taken to occur where there is merely an inquiry in order to ascertain facts or make a preliminary assessment of the nature of the matter. Rather, there must be an inquiry into "whether there is a reportable situation"[2].

The draft Guide (RG78.51) reproduces a paragraph from the EM that says:

> "For example, after receiving a complaint from a client, if the licensee begins to look into the matter or take steps towards ascertaining whether a significant breach has occurred."

An unsophisticated reading of this paragraph could take it to mean that an investigation commences when, upon receiving a complaint, "the licensee begins to look into the matter". That interpretation would clearly be at odds with the law. Section 912D(1)(c) specifically refers to an investigation whose purpose is to "determine whether there is a reportable situation of the kind mentioned in paragraph (a) or (b)". This requires a degree of engagement with the specific issues relating to reportable situations that goes beyond initial inquiries about facts or initial assessments of the relevance of mandatory breach reporting.

The mere receipt of a complaint does not necessarily trigger that kind of inquiry from the outset. Complaints might, for example, not even involve issues that could give rise to a significant breach. Similarly, complaints could be based on mistakes and misunderstandings.

In our view, it is unavoidable that licensees make some kind of initial assessment of the facts surrounding a complaint or other incident to determine its nature and what, if any, further action is required. For example, if a licensee does some initial fact checking and correctly makes a determination that a complaint is based on a mistake or misunderstanding and there was no reportable situation, this should not be an "investigation" that on expiry of the 30 day threshold itself becomes a reportable situation.

In most cases this sort of initial assessment may involve communicating with staff or the customer - both of which are cited in the Guide (RG78.48) as indicia of an investigation. If this was the case, virtually all complaints that were not resolved in 30 days would become reportable situations. Accordingly, it would be helpful if the regulatory guide made it clear that an investigation is not taken to have commenced on:

- the receipt of a complaint;
- the making of a compliant to AFCA;
- the initial factual and legal analysis of a complaint;
- the initial steps in a licensee's internal dispute resolution processes; or
- participation in the AFCA dispute resolution process.

Instead, investigations should be taken to have commenced only after the initial assessment of facts indicates a real possibility that a reportable situation may have arisen, and the licensee decides to proceed to collect facts to determine whether such a situation exists (if it is obvious that a reportable situation exists at this point, then, as the draft Guide states, the situation will be reportable without the need for an investigation (RG 78.57)).

Clarification of the above in the guide, potentially by way of example, would be welcome.

[2] Section 912D(1)(c).

1.3.2 Time of completion of an investigation

Similarly, certainty around the time of completion of investigations would be helpful. The Guide could, for example, clarify that an investigation within the meaning of s 912D(1)(c) is complete once it is decided whether a reportable situation has occurred, and does not, for instance, require conclusions as to the quantum of consumer loss or numbers of customers impacted by the breach, to be regarded as complete.

2. Deemed significance

2.1 'Material loss or damage' RG 78.38 – 39, Table 2

While we support the requirement to report breaches that involve material loss, we have consistently pointed to the difficulty and arbitrary nature of determining when this occurs. The draft Guide, however, does little to inform licensees, beyond what has been set out elsewhere, such as the Act and Explanatory Memorandum. While these are of course key sources of information, some further exposition of ASIC's view of the issue would be helpful. This might include some more examples of scenarios (including examples of scenarios involving wholesale clients) explaining in each instance whether ASIC would likely consider the loss material and why.

The need for further examples is all the more necessary in light of the requirement to consider materiality in the context of the individual customer circumstances. This entails a highly subjective process that could be interpreted differently among licensees. Guidelines as to how and when licensees should apply this criterion would help ensure consistent application of the relevant provisions.

Further guidance could indicate whether licensees are to consider the type of customer (e.g. individual vs large corporate) or additional matters like whether the customer is in hardship/financial distress (which would add additional overlay to processes to quantify the number and value of customer impacts).

Non-financial loss or damage

There are no examples in the guidance on what constitutes material non-financial loss or damage. Further guidance on this will assist licensees to determine:

- The significance of and/or the need for further investigation into whether non-financial loss is of itself material.
- Where, in conjunction with financial loss, a non-financial loss may be deemed material.

High-level guidance on what is non-financial loss similar to that provided by AFCA would be useful.[3]

2.2 Criminal offences

As noted in the draft (RG 78.37), breaches that constitute the commission of a criminal offence (punishable by specified periods of imprisonment) are deemed significant. The way the Act is drafted in this respect provides that a reportable situation arises only where a licensee 'reasonably knows or is reckless as to whether' there are reasonable grounds to believe that all relevant physical and fault elements are present. This is obviously going to be a higher threshold than for strict liability offence breaches or civil penalty breaches that do not have fault elements.

The Guide could benefit by ASIC setting out its approach on where a licensee should consider that reasonable grounds exist to believe that the breach constitutes 'the commission of an offence'. In particular, the Guide should confirm that if the licensee is satisfied that the necessary mental fault element/s for any deemed significant criminal offence is not present, there is no reporting obligation just because the physical elements of the offence are present.

These same considerations apply in respect of the core obligation relating to serious fraud.

[3] A copy of AFCA's approach to non-financial loss claims can be found here: https://www.afca.org.au/media/335/download

In our view, the Guide should also at least confirm that breach reports made by reason of these provisions will be taken only as indicating the presence of reasonable grounds to believe and not as an admission that an offence has been committed, for the purpose criminal proceedings. Inclusion of this in the Guide might reduce the need for licensee to include disclaimers in individual reports.

We also note that inclusion of this additional guidance is consistent with the decision of the Federal Court in *Australian Prudential Regulation Authority v Kelaher* [2019] FCA 1521, which found that statements contained in breach notices lodged with APRA did not constitute admissions for the purposes of court proceedings.

2.3 Civil penalty provisions

As noted above, a feature of the new regime is that breaches of civil penalty provisions are to be deemed significant. While the scope of this is subject to the yet to be finalised regulations, it will remain broad, such that determining which provisions are in scope will itself be a resource intensive task for licensees – including those with more limited resources.

For these reasons it would be helpful for ASIC to detail as an appendix to its Regulatory Guide the relevant civil and criminal penalty provisions in the legislation which are subject to the deemed significance provisions.

In addition, we consider that it would be helpful for ASIC to specifically include some examples of breaches that are reportable because of failures to comply with enforceable provisions of RG271 (assuming these are not excluded from deemed significance by the regulations). Failures to comply with RG271 are deemed significant by virtue of ss 912A(1)(g) and 912A(5A), Corporations Act and ss 47(1)(h) and s 47(4) of the Credit Act.

2.3.1 Exclusions in the Breach Reporting Regulations

As noted in CP340, the Government has consulted on draft regulations specifying the civil penalty provisions excluded from 'deemed significance' under s912D(4)(b) of the Corporations and s50A(4)(b) of the National Credit Act. The ABA made a submission in response to that process and we do not intend to reproduce the points made here.

However, we note that important considerations may arise when the regulations are finalised that may have relevance to ASIC's RG 78. We outline some examples below of provisions that we have suggested should be excluded from the 'deemed significance' applying to civil penalty provisions. In our view, the content of RG 78 may need adjustment according to whether or not the final regulations include reference to them.

Licensing obligations: general

The general licensee obligations listed in section 912A(1) of the Corporations Act and section 47(1) of the Credit Act (which include, for example, the obligation to do all things necessary to ensure that the financial services or credit activities covered by the relevant licence are provided efficiently, honestly and fairly) cover a very wide range of conduct. These provisions are among those that we have submitted should be excluded from 'deemed significance' by the regulations, primarily on the basis that their very broad scope necessitates the application of a significance threshold if ASIC is not to be inundated with reports of trivial breaches.

If the regulations exclude these provisions from deemed significance, they will nevertheless remain 'core obligations' under the new regime and it would be useful if ASIC provided guidance on its views of the circumstances in which breaches of these provisions should be regarded as significant, and include some examples.

Licensing obligations: 'Other legislation'

The general licensing obligations in the Acts also include the obligation to 'comply with financial services laws (or credit laws). These provisions are not, of themselves, subject to civil penalties, and so are not deemed significant. However, the obligations also cover the provisions of other legislation,

because of the effect of the definition of 'financial services laws' in the Corporations Act and 'credit laws' in the Credit Act.

A notable difference between the two Acts is that the Corporations Act provision on core obligations captures 'other Commonwealth legislation covering conduct relating to financial services' only where the relevant legislation is specified by regulations[4]. The Credit Act core obligation provision doesn't replicate the requirement for regulations, so that it extends to other Commonwealth legislation covering credit legislation without the prerequisite that it be prescribed in regulations.

We have drawn to the attention of the Government the question of whether this was intended, or was an oversight. We have also submitted to the Government, during its consultation on the regulations, that any civil penalty provisions of 'other Commonwealth legislation' brought into the scope of the deeming provision by operation of the above provisions, should be captured by the list of exclusions.

For present purposes, whether or not civil penalty provisions of other Acts are captured by the exclusions in the regulations, ASIC should clarify in RG 278 that it will read the phrase "only in so far as it covers conduct relating to the provision of financial services" in the relevant definitions[5] strictly, covering only provisions are directly and relevantly related to the provision of financial services (for the Corporations Act) or of credit (for the Credit Act), and potentially include examples.

To illustrate the risk we are here seeking to address - there are many other Commonwealth laws that licensees may need to comply with in the course of their business. If they are required to consider all of the provisions of these laws for either application of the significance test, or of the deeming provisions, the task will be very onerous. This is all the more the case for credit licensees as, at least as it stands, the set of 'other Commonwealth laws' that are relevant is not limited to those prescribed in regulations.

The Corporations Act provision will be limited to the list of Acts specified in the regulations, which does not include the Privacy Act, or the Anti-Money Laundering and Counter Terrorism Financing Act.[6] Under the Credit Act provision, however, these, as well as other Acts, are potentially in scope.

Consider the effect of the Privacy Act, for example, being in scope. An inadvertent instance of somebody sending something to the wrong address (be it mail or email), which contains only a name and address and poses no real risk of harm, could be reportable to ASIC, because it becomes a civil penalty provision (by virtue of section 13G), and so is deemed significant. There are a myriad of other minor/technical privacy breaches that could also be seen as 'repeated interferences with privacy' to which s13G of the Act could conceivably apply. A particularly anomalous result is that some minor breaches of the Privacy Act which are not reportable to the Office of the Australian Information Commissioner (OAIC), could conceivably be reportable to ASIC under this regime.

If deemed significance of this kind of provision is wound back by the regulations, licensees may still need to apply the significance test unless ASIC makes clear that it does not consider such provisions to cover "conduct relating to the provision of financial services" (see above). This would not rule out the possibility that some provisions of the Privacy Act (or other Acts) could be captured by the new reporting regime. We suggest only that this be clearly limited to provisions directly relevant to the provision of credit (and hence relevant to ASIC). In our view this is the better view of the effect of the legislation, but it would be helpful if this was put beyond doubt in the Guide.

It would also be useful for ASIC to clarify how the reporting obligations will apply in relation to other regimes such as the Banking Executive Accountability Regime (BEAR) under the Banking Act. For example, does reporting of a matter to APRA, or the OAIC, extinguish any obligation to report to ASIC under the Corporation Act regime.

[4] Corporations Act, s.912D(3)(c), s761A(d).
[5] See paragraphs (d) of the definition of financial servicers laws in section 761A of the Corporations Act and of 'credit legislation' in section 5 of the Credit Act.
[6] See regulation 7.6.02A of the Corporations Regulations (and note that the regulations recently consulted on will apply that same list under the new regime – see item 5 of the Financial Sector Reform (Hayne Royal Commission Response—Protecting Consumers (2020 Measures)) Regulations 2021: breach reporting (Exposure draft)

Australian Banking Association

3. Reporting of multiple breaches related to a single cause or systemic issue

3.1 Guidance on breaches with multiple related scenarios or instances

It would be helpful for ASIC to provide further guidance on how to report reportable situations in which multiple scenarios or instances may be related or linked. For example:

- whether separate breach reports are required for multiple breaches of a civil penalty provision with the same cause, or where a number of representatives are involved in the one breach or have committed similar breaches; or
- whether a separate breach report needs to be lodged where a licensee has reported a reportable situation, and subsequently identifies further instances arising from the same root cause, having similar facts and/or breaching the same obligation.

An example of the second point is where a fee is charged in error with respect to product 'A' due to a system deficiency and subsequent to reporting this to ASIC, it is identified that the same fee charging error has occurred with respect to product 'B' (separate products).

Another example of the second point (but with a single underlying product) would be where the licensee reports a systemic issue of overcharging a certain fee (e.g. X fee) on a particular product (e.g. Y product). If the licensee is not able to immediately stop overcharging X fee on Y product and the matter is deemed significant, clarity should be provided as to whether the licensee is required to report each subsequent overcharging incident for each customer, or to report separate breaches until the issue has been fixed.

The Guide could clarify that it is sufficient if these additional instances be added to the initial breach report by way of an update. An approach that requires licensees to report each subsequent individual instance would only exacerbate the likely problem of a large volume of reports, making it difficult for ASIC and licensees to focus on the significant issues.

3.2 Guidance on the provision of updates to previously reported matters

The Guide states (in RG78.88):

> "After you report an ongoing investigation to us, we expect you to update us if before the investigation is completed you become aware of a material change—for example, where the investigation reveals further information about the scope, nature or cause of a possible breach."

It would be helpful for ASIC to provide further guidance on expectations relating to updates to previously reported matters, in particular:

- whether ASIC requires updates for every breach report, or only certain reports at ASIC's discretion. If so, what factors will ASIC take into account in exercising its discretion; and
- the timeframes or frequency for providing updates.

Examples highlighting ASIC's reporting expectations could include:

- submitting a report providing all the reportable situations at the end of the (30 day) investigation; or
- submitting multiple reports immediately as soon as the reportable situations are known during the 30 day investigation period, and providing information that a licensee is still investigating the 'same subject matter' or event for other possible reportable situations; or
- submitting ongoing regular updates to reports of additional information ascertained after the end of the investigation into whether a reportable breach has occurred (eg updated customer numbers and updated total estimated remediation amounts).

It would be helpful if this was clarified in the Guide.

It would also be useful if ASIC clarified what it expectations for financial services and credit licensees seeking to provide update post commencement of the new regime, in respect of matters originally reported under the current regime.

4. Reporting of advisers and mortgage brokers

In the context of reporting external licensees, further guidance and examples around what does and does not amount to 'reasonable grounds to believe' would be helpful. Licensees do not have an obligation to investigate potential misconduct by brokers / advisers that operate under an external licence. Therefore there are likely to be scenarios where the bank becomes aware of facts (such as the existence of an undeclared liability in a credit application) and there are several possible explanations, ranging from human error, customer misconduct or broker misconduct. In the absence of an obligation to investigate, presumably where there are several explanations that would be believable to a reasonable person there is no obligation to report. It would be helpful to have an example of a situation where ASIC does not think the obligation to report an external licensee arises.

At times, consumers may direct their complaints to the incorrect licensee. For instance, making a complaint about a mortgage broker's conduct to the lender. It will be helpful if ASIC could include an example for this scenario, setting out ASIC's expectations of licensees in relation to reviewing misdirected complaints about advisers and mortgage brokers.

It would be helpful for ASIC to acknowledge the role of aggregators in facilitating the provision of credit to clients. Lenders generally have a contractual relationship with the aggregator, who accredit and manage the broker. The lender will authorise the broker to sell its products.

More specifically, it would be beneficial if ASIC could provide guidance where:

- An Aggregator is unhelpful in addressing broker misconduct (where the broker is a credit representative of the Aggregator). The example in Table 7 could provide further detail in terms of any further action the reporting licensee should take (ie. should the licensee report the Aggregator to ASIC?).

- An Aggregator is not a licensee for the broker as the broker holds their own ACL, and the breach report is to be provided to the broker, but the broker is not appropriately addressing the conduct concerned.

It would also be useful to see some examples for credit licensees on:

- best interest duty obligations and interactions of this with the breach reporting regime – particularly in Table 7, page 26, and
- examples of material loss and damage requirements in Table 2, page 15.

5. Reporting in the prescribed form via the ASIC Regulatory Portal

We note that ASIC's regulatory portal will play a key role in the operationalisation of the new breach reporting regime. We note that we have raised concerns with ASIC about the functionality of the portal, especially the absence of a capability to accept batch reporting of breaches. We would welcome further engagement with ASIC on the operational aspects of the portal prior to the new regime taking effect in October. It would also be helpful if ASIC's planning included a period of testing of the breach reporting aspects of the portal prior to the new regime's commencement.

We set out some key issues identified by our members in relation to the portal below.

5.1 Information required at time of report

Licensees may not always have a complete set of information at the time that they lodge a report. For this reason, we suggest that the portal should be designed so that a licensee is able to provide the information that it does have access to at the time of reporting – with acknowledgement that a licensee may not have all the information at that time.

If this suggestion were adopted, it would require that most information fields be optional rather than mandatory, so that not all fields would be required to be completed where not all information is reasonably attainable at the time of reporting. Alternatively, there should at least be an option to populate the fields with 'unknown' or 'under investigation' so that the information can be updated once identified.

5.2 Opportunities for enhanced efficiency of the portal

We note that ASIC has release wireframes for the portal for review by key stakeholders. Overall it appears that the draft wireframes contemplate the provision to ASIC of more data per reportable situation than is presently the case. Bearing in mind the anticipated significant increase in the volume of reporting likely under the new breach reporting laws, and that there is no ability for licensees to automatically upload (or batch) reports into the ASIC portal, we submit that all opportunities to reduce the costs and burden of reporting and providing updates be explored. Some examples of opportunities to reduce the burden of reporting and providing updates include:

- Minimise free text fields - There are a number of free text fields in the wireframes. We consider that free text fields should be minimised. We have provided separate feedback to ASIC on the particular free text fields we think warrant consideration about whether there are alternative and simpler means of obtaining information. We have recommended that ASIC reconsider the number of free text fields, and instead use pre-determined fields for everything other than the description of the event.
- Previous similar reportable situations - We are concerned that the current approach to P2-S4-4 and P2-S4A-4, which require the identification of "similar reportable situations (that do not form part of this report) previously occurred" is potentially unachievable. In light of the potential for a significant increase in reportable situations for relatively simple, yet isolated, breaches (e.g. responsible lending), the number of 'similar events' could run many instances (possibly hundreds) and the wireframe indicates ASIC will require details of previous reports of all of these events. We would ask that ASIC consider an alternative approach here or to remove this requirement.

Further, the operation or logic of the wireframes is unclear in certain situations. We consider that further guidance or clarity could be provided in the following situations:

- Reporting outcomes of ongoing investigations - An event that is reported as being investigated may identify two (or more) legal breaches, but, after further investigation one is found not to be a breach. The draft ASIC portal wireframes do not appear to allow for the two (or more) different outcomes in an investigation.
- Reporting more than one reportable situation - Where a breach report relates to more than one reportable situation, for example, a breach of a core obligation and an additional reportable situation (as illustrated in Example 6(a) of draft Regulatory Guide 78), does ASIC expect that each type of reportable situation be identified in the "nature of the reportable situation" section of the prescribed form?
- Updating breach reports: The wireframe appears to only allow for updates to a breach report itself where there is an ongoing investigation (P2-S1-6) or a likely significant breach (P2-S1-17) (reporting when that breach eventuates). This suggests that if further affected customers or breaches (relating to the same event) are identified, and the report is closed to further updates (eg. there is no open investigation report) these would have to be lodged as a new report.

- Similarly, if serious fraud and/or gross negligence were discovered during the course of banks' post-reporting investigation (eg. there is not an open investigation report – as this would be captured in P2-S1-10), it would appear more efficient and practical to be able to update the report rather than needing to lodge a new report.
- Other aspects of the portal would benefit from clarification, either in the Guide or elsewhere. For example:
    - We note that in the portal the terms 'remediation' and 'rectification' are used interchangeably as equivalents. It would be helpful to understand whether ASIC intends rectification to occur when the remediation concludes.
    - Within the portal, ASIC asks "are you aware of any action or proposed action by the other regulatory body in relation to the breach?" It would be useful if ASIC clarified whether 'action' here is intended to mean enforcement action or litigation, or broader regulatory action (for example a request for information).

We do not consider that any additional information should be captured in the prescribed form. We note that the information captured by the portal is more than sufficient to understand the reportable situation, the nature of breach, the extent of breach, and its rectification and remediation.

5.3 Volume of information required to be reported

We note that the proposed amount of information required to be entered into ASIC's portal has increased from the existing requirements, along with an anticipated significant increase in the volume of matters that will require reporting to ASIC as a result of the legislative changes. This will require substantial increases in scarce compliance resources, and associated costs, particularly given it must be done within the 30-day time period and that there is no ability for licensees to automatically upload (or batch) reports into the ASIC portal (see below).

This highlights the importance of the suggestion above regarding opportunities for efficiencies in the way information is collated by ASIC through its prescribed form and the portal.

Analysis by one of our members indicates that currently, data for each reportable incident takes at least 30 minutes to lodge via the ASIC portal. Depending on the features of the new breach reporting portal, the time to report a single incident may well extend beyond this. If a bank has thousands of reportable incidents in one year under the new regime (where currently they may report a hundred or less) – a conservative estimate for some of our members, it would need to invest approximately 2,500 additional hours of scarce compliance resources on data entry into the portal.

Currently the ASIC portal is only able to accept individual, manually entered breach submissions. It would be helpful if ASIC could improve the efficiency of uploads to the portal (eg through daily batch reporting) to reduce the manual work required to lodge individual breach reports.

5.4 Liability of the submitter on ASIC's portal

The declarations (on the existing portal) that the person performing the role of 'submitter' must make, appear to expose individuals to an increased risk of civil and criminal liability. This occurs where the staff member, performing the role of a 'submitter', is compelled to respond to each question regardless of whether banks have the required information at the time of submission.

Especially in larger banks, duties associated with breach reporting may be centralised or delegated. Staff involved in collating and sending the notification to ASIC, and coordinating the response to requests for updates may not be personally aware of every piece of information required by the portal. The 'submitter' role in the portal appears be more administrative (associated with collating and submitting the breach report) but then appears to apply individual responsibility for the content of a breach report (through the mandatory declarations).

Given the significantly increased volume of breach reporting expected post 1 October 2021, and the 30-day time period for reporting, we will need to delegate this 'submitter' role to a wider group of employees than is currently the case. Having individual liability on the 'submitter' also limits the ability of licensees to use technology to automate some of the data entry process.

We do not think it is necessary or appropriate to impose that personal liability on an individual acting in the 'submitter' role. We suggest that ASIC could direct the declaration at the reporting entity as opposed to the individual.

5.5 Ongoing communications

Relevant to the role of the 'submitter', we also note that there is opportunity for efficiencies in managing ongoing communications between ASIC and licensees. We note that the ASIC Portal's current functionality requires the individual performing the 'submitter' role to be the key contact when emails are sent from ASIC advising of a message in the Portal. This risks messages being missed as staff who have previously been a 'submitter' will take leave, change roles or leave their bank. With the significant anticipated increase in the volume of reporting, it is likely that more individuals within banks will be submitters, exacerbating this issue. We also see value in people other than the submitter being notified of messages relating to a matter. To avoid this, we suggest an option of using a centralised mailbox.

We also note that it would be helpful for the messaging facility in ASIC's portal to remain "open" for all breach reports to ASIC (at least until the matter is considered closed or no further action is required). We have found the messaging facility is closed for some but not other events.

5.6 Specific questions on ASIC's draft Portal Form Design Document

We have some specific queries regarding the questions in ASIC's draft Portal Form Design Document. We list the relevant parts of the document and our associated questions below:

- "Summarise the results of the investigation into whether the breach had occurred/you were no longer able to comply with the core obligation."
    - What information is ASIC seeking in this question that is not already covered in the form?
- "Have any similar reportable situations (that do not form part of this report) previously occurred?"
    - Is the reference to 'similar reportable situations' to all types of reportable situations or just 'core obligation' breaches? And is it limited to reportable situations post 1 October 2021?
- "Have you compensated all clients .." and then "If Not started, Do you intend to compensate clients?"
    - As to the second part of this question, is ASIC asking "Do you intend to compensate all clients?" or "Do you intend to compensate any clients?"
- "Specify the total dollar amount you paid in compensation to clients"
    - Should the response to this question also include any amount paid to unclaimed money?
- "Specify the number of clients you compensated".
    - The number of clients compensated will not always reconcile with the number of clients who suffered a loss (eg. customers unable to be contacted and paid and customers considered out of scope for remediation payment). How does ASIC propose to treat this information?
- "Provide a description of your handling of the reportable situation"

- The draft RG does not give guidance on ASIC's expectations for responding to this question. The Note in the Portal Form duplicates other questions already answered. How does ASIC propose to treat this information?

- "*Have the person/s alleged to have been involved admitted to the conduct?"*
  - This Yes/No question may be difficult to answer in a timely manner given the nature of the allegations and the potential legal ramifications for making any admission in the form.
- "*.. the total number of clients the reportable situation affects*" and "*.. the total financial loss to affected clients*".
  - ASIC notes that if the investigation is complete the response cannot be an estimate and the licensee is expected to know the total numbers. This is not always feasible as the investigation into the issue may be complete (eg. determined there was a significant breach of a core obligation) but identifying the final number of customers and any financial impact can take many months. How should this be reported (ie. investigation not complete)? If the licensee reports that the investigation is not complete for several months to finalise these figures, what will ASIC's approach be?

6. Complying with the notify, investigate and remediate obligations (Draft information sheet)

6.1 Separate information sheet, or incorporation into RG 256?

We submit that ASIC's guidance on the new notification, investigation and remediation of breaches obligations should be incorporated into RG 256. By having a consolidated document on remediation policy would assist firms to achieve clarity and apply the regime without uncertainty of requirements.

6.2 What should be included in notices to affected clients?

We note the initial notification is required to be provided before an investigation has been completed, and in some cases before the breach has been confirmed. For this reason, we suggest that ASIC consider re-wording the term "breach" to "reportable situation" in these instances.

It is important to note that, as licensees must give the initial notices to the impacted clients at an early stage, the licensee may not always know whether the customer has suffered a loss, the quantum of loss, and whether any compensation will be offered.

The Information Sheet does not outline the ACL holder's obligations to notify the impacted lenders or aggregators of the investigation and remediation. We submit that this should be expressly called out in the Information Sheet.

Does ASIC intend to require "rolling" notifications to customers? The s912EA notification obligation arises in respect of each affected client (compare to the notification obligation under s912EB(5), which starts after the completion of the investigation). For some factually complex scenarios, a licensee may uncover newly discovered tranches of 'affected clients' in staggered stages (i.e. different points in time). Clarification of how ASIC envisages how licensees would meet the s912EA notification obligation under these circumstances would be helpful.

The form for providing the required information to affected clients need not, in our view, be approved by ASIC.

Guidance on "reasonable steps" to notify and remediate affected clients

Guidance on what are "reasonable steps" to notify and remediate affected clients in the scenario where the licensee does not have contact information for the client would be helpful. Also, confirmation that, where reasonable steps are taken to put systems in place in preparation to notify and remediate but

those steps are not actually taken within 30 days, the requirement has nevertheless been met. This might be the case, for example, where large numbers of customers are affected.

We note that ASIC recently consulted on its updated Regulatory Guide 256: Customer Remediation and proposed that licensees apply "best endeavours" to find and pay consumers. It would be helpful to understand whether ASIC's expectations for "reasonable steps" under the draft Information Sheet are the same as its proposed "best endeavours" under RG 256 in relation to notifying and remediating affected clients where the licensee no longer has contact information for the client(s).

7. Transition

It would be helpful if the Guide addressed the transitional approach as it applies to credit licensees, with examples. In addition, the document could provide:

- Further guidance and an example where an investigation is commenced under the old regime and what types of activities could require an existing incident to be considered under the new breach reporting requirements, particularly as they relate to investigations.
- Guidance on what obligations exist for incidents which have been previously assessed under the regime pre 1 October 2021, and then reassessed post 1 October 2021.

Guidance on the transition of the application of the Info Sheet to existing remediation programs would be beneficial. For example, where a significant breach is reported under the current regime and clients are being remediated, but during the course of that remediation after 1 October 2021 additional affected clients are identified who have incurred a recoverable loss, should the Info Sheet apply to that newly identified cohort of impacted clients or should they be remediated as part of the existing remediation program?