



FINANCIAL
SERVICES
COUNCIL

ASIC Consultation Paper 340 - Breach Reporting and related obligations

Financial Services Council Submission
7 June 2021



Contents

1. About the Financial Services Council	3
2. Introduction	3
3. General Comments	3
4. Specific Responses to the proposals and questions in the Consultation Paper	5

1. About the Financial Services Council

The FSC is a leading peak body which sets mandatory Standards and develops policy for more than 100 member companies in one of Australia's largest industry sectors, financial services.

Our Full Members represent Australia's retail and wholesale funds management businesses, superannuation funds, life insurers, financial advisory networks and licensed trustee companies. Our Supporting Members represent the professional services firms such as ICT, consulting, accounting, legal, recruitment, actuarial and research houses.

The financial services industry is responsible for investing \$3 trillion on behalf of more than 15.6 million Australians. The pool of funds under management is larger than Australia's GDP and the capitalisation of the Australian Securities Exchange and is the fourth largest pool of managed funds in the world.

2. Introduction

The FSC welcomes the opportunity to make a submission to the Australian Securities & Investments Commissions (**ASIC**) in relation to the *Consultation Paper 340 – Breach Reporting and related obligations (CP340)* and Draft Regulatory Guide 78 *Breach reporting by AFS licensees and credit licensees (RG 78)*.

Please note that this submission does not cover all the questions raised in CP340 but only provides some general comments and specific comments in response to nominated questions below based on feedback from FSC Members.

3. General Comments

The FSC raised the following general comments/queries:

1. A key issue for FSC is timing: we note consultation is intended to help industry make changes and improve practices before the reforms commence on 1 October 2021. ASIC intends to release the final RG 78 "before" the reforms commence but has not indicated a definitive timeframe. In order for industry to have time to consider and implement any necessary and appropriate changes before the reforms commence, we would be grateful if ASIC could finalise its guidance at least two months before the new law commences on 1 October 2021. These changes include changes to training, processes, procedures and underlying system changes in preparation for the new regime. They can be very time consuming and can only be finally scoped once the updated RG 78 and information sheet are released.
2. Another key concern of FSC and its members is the lack of a significance/materiality threshold or requested relief from certain parts of the civil penalties regime within the breach reporting framework. The concern is that there is a real risk of added substantial costs for the financial sector and a major proliferation of technical breaches to be processed by ASIC. We note that this could well result in a significant increase in the volume of breach reporting take away the focus of all stakeholders from more serious breaches, leading ultimately to a further undermining of the integrity of the sector.

3. FSC and Member concern has also been expressed on practicality of the implementation of the new breach reporting regime coinciding with the introduction of other new regulatory changes in the next 12 months, notably including:
 - a. Design and Distribution Obligations (**DDO**);
 - b. Commencement of annual renewal of ongoing fee arrangements
 - c. Advice fee consent and independence disclosure requirements
 - d. Introduction of the single disciplinary regime for financial advisers.
4. In this regard, a good example of a foreseeable source of a significant increase in the volume of breach reporting arises from an unfortunate interaction between the new breach reporting and DDO regimes. In short, where a licensee becomes aware of another licensee's breach of DDO requirements, when applicable, for example late reporting of complaints numbers, this would trigger the so called "dobbing regime" duty to report the breaching licensee's breach. The only exception to this requirement would be if there were reasonable grounds to believe that ASIC had already been fully informed of the breach. Further details of this scenario are set out below.
5. Members are also concerned about what ASIC will publish. In this regard we note that Paragraph 11.123 in the Explanatory Memorandum (**EM**) includes the following reference: "ASIC will be required to publish this information on its website within **four months after** the end of each financial year, starting on the financial year ending on **30 June 2022**". On this basis, the first ASIC publication will be in early Nov 2022. Could ASIC please clarify if the intention is for the first publication will include breaches for the full 12 months ending 30 June 2022? If so, we note that such a period would begin from 1 July 2021, whereas the new breach laws start 1 October 2021.
6. Members have concerns regarding the prescribed form. It is felt the proposed form outlined in RG 78 is a "one size fits all" form and would result in licensees not being able to provide all of the information in every circumstance because of the different nature of reportable situations. For instance, the reporting of an ongoing investigation is unlikely to include information about steps taken around rectification and or client remediation, or information about steps being taken to ensure future compliance. This would result in multiple follow-up communications to ASIC and administrative complexity.
7. Members have widespread concerns about the ASIC Regulatory Portal (**Regulatory Portal**). We note the FSC requested to consult with ASIC on the proposed ASIC Regulatory Portal enhancements. In this regard, the FSC sent a list of issues to ASIC in relation to the new breach reporting regime ("**List**" attached as **Annexure 1**) and while we had verbal feedback on the List, the Regulatory Portal related issues were not discussed due to unavailability of relevant ASIC personnel (see in particular paragraphs 11 to 17 of Annexure 1).
8. Members would appreciate more guidance regarding the meaning of certain key terms such as "investigation", "material loss or damage", "gross negligence" and "reasonable grounds to believe".

4. Specific Responses to the proposals and questions in the Consultation Paper

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 situation.

B1Q1 - Do you agree with our proposed approach? If not, why not?

Yes. Our expectation is that licensees will continue to be consulted on proposed guidance.

B1Q2 - Are there differences in the structure or operation of credit licensees that require specific guidance on how the breach reporting obligation applies?

We note that there will be licensees who hold both an Australian financial services (AFS) licence and credit licence; being able to apply the same principles/process where appropriate will assist with compliance with the breach reporting obligations.

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 Are there any specific issues, incidents, challenges or areas of concern you think we should include as examples, case studies or scenarios? If so, please provide details and explain why they should be included.

Certain of our Members feel that the concept of “core obligations” creates some uncertainty and risk for licensees operating authorised representative models. This is on the basis that on one view, it is not clear if it is possible for an authorised representative to contravene the obligations contained in 912A of the Corporations Act of the Corporations Act 2001 (Cth) (the **Act**), although the guidance is framed in a manner that suggests licensees’ reporting obligations may be triggered by authorised representative actions that do not strictly breach the core obligations. It would be helpful if ASIC could provide some guidance on this point.

See also replies below to B4 and B5.

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.

B3Q1 Should we include further guidance to help AFS licensees understand how the existing breach reporting obligation under s912D of the Corporations Act (as in force before 1 October 2021) applies? If so, please provide details.

The guidance provided is useful and Members have indicated that they do not require further clarification in this regard.

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 Do you agree with our proposed approach? If not, why not?

Yes. Members would like to continue to be consulted on proposed guidance.

B4Q2 Should we include further guidance on what constitutes a ‘core obligation’? If so, please provide details.

The perceived anomaly referred to in the above response to B2Q1 should be addressed by the guidance text

B4Q3 Should we include further guidance on how to determine whether a breach or likely breach of a core obligation is ‘significant’? If so, please provide details.

Yes, our Members expect continued engagement on the nature and content of that guidance. We note that Table 5 provides examples of breaches that may not be significant, and the main example provided is “Isolated failure to give a disclosure document (Financial Services Guide (FSG)) or Credit Guide”. Members feel this is not an especially helpful example given this is covered by the (draft) regulation as an excluded civil penalty provision. Further examples of breaches that may not be significant would be useful.

Whilst a matter for Treasury, we also want to raise again in this regard the concern that a breach of s601FC of the Act (e.g. any breach of compliance plan) will trigger a civil penalty provision. This is noted under Example 2(d) of RG 78.

However, many of these compliance plan breaches will be minor, inadvertent and administrative in nature and generally will have no detriment to the unit holder – for example, failure to lodge compliance plan audit opinions timely, failure to lodge financial reports timely, distribution of scheme financial reports to Members timely, unit pricing error in which the Member actually benefits.

Notwithstanding that some of these breaches could be considered as significant under s912D(5) (e.g. number or frequency of similar breaches, or inadequate compliance arrangements), on their own these would not be considered as deemed significant breaches under s912D(4)(b) and Members are concerned this would create additional strain on both licensee and ASIC resources if reporting obligations were to be triggered.

B4Q4 Should we include further guidance on reporting an ‘investigation’ to ASIC? If so, what should be clarified? Please provide examples of scenarios (where relevant).

Yes. We note that while RG 78 restates Treasury’s guidance in the EM, it would be helpful if it provides additional clarification and guidance (preferably by way of a clear definition) as to what constitutes an “investigation” to enable greater consistency of approach among industry, particularly regarding when an investigation is considered to have commenced.

For example, we refer to Example 5(a) at Table 6 of RG 78 which is used to illustrate examples of investigations which are reportable. The example helpfully states that the internal audit which revealed the unit price error itself is not reportable because it is routine and not directed at identifying whether a significant breach of a core obligation has arisen and so it does not constitute an investigation. Generally, our Members feel that the existing examples in Table 6 are useful in assisting with understanding when an investigation might commence. We consider that it would assist the industry if ASIC provided some further examples of the types of matters that would not, of themselves, be considered investigations and therefore not reportable - similar to Table 5 on page 20, which has examples of breaches that may not be significant.

To that end, there are two areas of uncertainty where ASIC clarification is requested and like audits, form part of licensees' regular and routine compliance practices, namely:

- a. The **"end to end management"** (including the investigation component) of a customer complaint through the licensee's internal dispute resolution (**IDR**) process in accordance with RG165 (and RG271 to commence on 5 October 2021); and
- b. **"Quality assurance monitoring"** in line with, for example, section 4.4 of the Life Insurance Code of Practice or otherwise.

Members are concerned with the anticipated increase in the volume of investigations that would be reportable under the new regime and the potential for inconsistent application of the law if these two areas are not clarified in RG 78 as being not reportable. Therefore, it would be helpful if ASIC could provide some examples in its RG 78 to confirm that an IDR investigation and quality assurance monitoring are prima facie not of themselves reportable situations, with the appropriate carve outs to capture the Parliamentary intent of the new regime. A suggested example could read as follows:

A customer complaint that is managed and investigated as part of a licensee's internal dispute resolution process or external dispute resolution processes is not reportable.

However, if the complaint:

- (a) reveals that there is a breach (or likely breach) of a core obligation that is significant then it would likely be reportable to ASIC; or*
- (b) triggers a subsequent investigation into an issue identified as part of the original IDR investigation i.e. non-compliance with a financial services law that relates to multiple clients then this may suggest a systemic issue and the investigation into the systemic issue would likely be reportable to ASIC if it continued for more than 30 days.*

We note that Case Study on page 22 of RG 78 1 appears to align with this rationale.

In addition, at RG 78.51, ASIC provides an example of when an investigation of a complaint might be deemed an investigation for the purpose of the breach reporting requirements. Could ASIC clarify the intent behind 78.51 and whether any open complaint exceeding 30 days would require reporting to ASIC, even in the instances covered by RG 271.63 to 271.68 (dealing with IDR)?

As to timing concerns in the context of investigations, Members would like to stress that timing requirements need to have regard to the inherent challenges of preliminary information gathering which may require engagement with clients, external third parties and legal representatives. Failure to allow sufficient time to conduct those activities has the potential to unduly impact individual advisers and clients and to create an unhelpful volume of reporting of insignificant matters.

B4Q5 Should we include further guidance on what constitutes 'material loss or damage'? If so, what are the challenges licensees face in determining whether loss or damage is material? Please provide examples of how you consider questions of material loss or damage.

Yes. Additional guidance on materiality of loss would be useful. The guidance should be principles based and have regard to both quantum (preferably by providing monetary thresholds) and relativity to business size and scale and client circumstances. Examples of non-financial loss or damage would also be useful, together with guidance / scenarios as to how these would be determined to be material.

We note that Section 912D(4)(d) of the Act deems breaches that result in, or are likely to result in, material loss or damage to clients or Members of a scheme or superannuation fund as significant. We refer to RG 78.38 of RG 78 which states that it is sufficient for significance to be established if the breach is likely to result in material loss or damage to one person and that a relevant circumstance in determining whether the loss or damage is material for an individual is the customer's financial situation.

It would be helpful if ASIC would provide additional information to clarify the following in RG 78:

- a. Include a *material loss and damage monetary threshold* for an individual and an aggregate monetary amount for a cohort of affected customers. This would provide context in relation to how ASIC will apply "extensive" which is the ordinary meaning of material as referenced by Treasury in the EM; and/or
- b. *Include monetary amounts* in the examples set out in 2(a) of RG 78 in relation to the financial loss suffered, so it is clearer to industry how ASIC will consider materiality in respect to an individual and an aggregate of customers/members as stated above. If it is not possible to provide any monetary thresholds on 'material loss or damage', we suggest that ASIC supplements with additional examples and cases studies whereby the incident, involving a mixture of retail and wholesale clients, constitutes as being 'material loss or damage'; and/or clarify
- c. *what other factors should be taken into account* when determining what is material loss or damage – we note that financial service providers would often not be aware of the customer's financial situation and would not consider this aspect due to the risk that it could be providing personal advice if the financial position of the customer is taken into account. It would be helpful if ASIC could confirm that in considering the circumstances of affected consumers, this can be based on the information that the licensee already holds/knows about the consumers. That is, licensees are not expected to contact the affected consumers and make inquiries about their circumstances for breach reporting investigation purposes. This is relevant in particular to ASIC's existing guidance where we note that in explaining what may amount to "material loss or damage," at paragraph 78.38, the RG makes reference to the EM. Whilst the material is useful in describing the concept, licensees are likely to find it challenging to apply in practice. For example, how is it possible for all licensees to know about each client's circumstances at a point in time? Also, how is a licensee to determine if a loss is material as each individual's circumstances are subjective and unique to each person?

Finally, some assistance could be obtained by considering basis point metrics – as you may know, general practice within the funds management industry considers errors greater than 30 basis point as deemed material and requiring compensation. This is consistent with ASIC/APRA's RG 94 Unit Pricing – guide to good practice. Is this also ASIC's expectation under the new breach reporting regime? Further guidance, examples, and case studies on the treatment of errors less than 30 basis point would be beneficial.

B4Q6 Should we include further guidance on reportable situations involving serious fraud or gross negligence? If so, what are the challenges licensees face in identifying when serious fraud or gross negligence has occurred?

Yes. Members raised concerns regarding the lack of definitions. In particular, the term “gross negligence” is not elaborated on within RG 78 and it would be helpful if ASIC provided guidance to explain and apply this term. Given there is no definition of gross negligence, we suggest that ASIC supplements with examples and case studies whereby the incident constitutes as gross negligence, gives rise to a reportable situation.

In addition, it would be useful for guidance and scenarios to assist licensees to understand the timing and circumstances for when these reportable situations are triggered by providing input on the following:

- a. Example scenarios that constitute gross negligence and serious fraud;
- b. guidance as to how and when an licensee determines they/a representative has engaged in conduct that constitutes gross negligence;
- c. further guidance on how/when it is deemed that the licensee/representative has committed serious fraud (is this only triggered after a conviction?); and
- d. guidance as to when licensees seek legal advice before concluding that conduct amounts to gross negligence;
- e. is gross negligence likely to fall within the definition of “serious compliance concerns” outlined in ASIC REP515 paragraph 108?

B4Q7 Should we include further guidance on reportable situations about other licensees? If so, please provide details.

Generally, it would be useful to receive practical guidance on situations in which this may arise. Members have raised concerns about reportable situations about other licensees including specifically:

- a. If an adviser or broker purchases someone else’s clients, do they need to review the entire client file to identify potential reportable situations to comply with this obligation?
- b. Is there a timeframe on how far an adviser or broker needs to look?
- c. What if the potential reportable situation has already been rectified and this occurred some years ago. Would this obligation still apply?
- d. How does a licensee satisfy itself that it has reasonable grounds to believe ASIC is already aware of an adviser or broker’s potential breach and has “all of the information that is required” (78.66)? Is “all of the information” based on breach Regulatory Portal requirements? What if those (Regulatory Portal) requirements change over time – could this trigger a report to capture a missing data point?
- e. Complaints: Often, consumers will incorrectly make complaints to lenders about the conduct of brokers. The complaint is either sent to the broker (if the consumer’s consent is obtained) or the consumer is referred to the broker’s IDR process. Similar to example 6(a): Falsification of loan application documents, it will be helpful if ASIC could provide an example for complaints about brokers that leads to a review by the lender.

- f. We refer to RG 78.90 which states that ASIC will contact the licensee if it requires further information about the report and this will generally be done through the Regulatory Portal. Does this mean that ASIC does not want to receive progress or status reports following the initial breach report and that licensees can assume that ASIC does not intend to take any further action if a Member has not received any request for further information?
- g. It would assist if ASIC provides guidance as to how it will manage breach reports for matters caught by the deeming test which result in trivial, administrative and small matters being frequently reported that do not cause loss or damage to customers. We note that the reforms may cause more matters of this kind to be reported and we understand that ASIC have not been consistent with their acknowledgement, request for more information and next steps.
- h. In the Appendix on page 44 of RG 78 ASIC has set out the relevant financial services laws that a licensee must comply with under section 912A(1)(c) of the Act pursuant to the definition of financial services laws in section 761A of the Act. Under subsection (d) of the definition of financial services laws a licensee must also comply with any other Commonwealth or State legislation that covers conduct relating to the provision of financial services as set out below.

“any other Commonwealth, State or Territory legislation that covers conduct relating to the provision of financial services (whether or not it also covers other conduct), but only in so far as it covers conduct relating to the provision of financial services.”

It would be helpful if ASIC could provide further guidance and examples of such legislation that would fall within this subsection.

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 Should we include further guidance to help licensees understand when to report to ASIC? If so, please provide details, including what guidance would be helpful and why

We note that RG 78.80 reads as follows:

To ensure you comply with s912DAA(3) of the Corporations Act or s50B(4) of the National Credit Act, you should not wait until after the following events to lodge your report:

- a. *the reportable situation has been considered by your board of directors;*
- b. *the reportable situation has been considered by your internal or external legal advisers (emphasis added);***
- c. *you have rectified (when appropriate), or you have taken steps to rectify, the breach (or likely breach) of a core obligation or additional reportable situation; or*
- d. *in the case of a likely breach, the breach has in fact occurred*

Concerns have been raised that this can have the effect of placing a licensee in a difficult position. The concern also arises of whether it would be procedurally unfair not to allow

licensees time to seek legal advice, having regard to the matters required to be ascertained/determined and the potential implications of reporting.

In particular, we note that the RG states at RG78.80 (b) that a licensee should not wait until after the reportable situation has been considered by its internal or external legal advisers. We understand that the intent of that guidance is to avoid reporting delays and to mitigate poor conduct such as where a compliance area provides a recommendation that a matter is reportable to ASIC that is subsequently not approved by senior management and therefore not reported. There is a view that a licensee should not wait until after a CEO or board of directors approves or agrees that a reportable situation has arisen. However, under the new regime a compliance area may not possess the legal skills necessary to accurately assess whether there has been a breach of law. The deeming significant test includes a list of criteria (save for material loss or damage) that requires an analysis of whether there has been a contravention of law and without legal training, a compliance representative may not be in the position to make a determination that a reportable situation has arisen, until after it has consulted with, or received advice from its internal or external legal team.

Members agree that if a compliance area has enough information or facts to know that a reportable situation has arisen, then it should not wait to report the matter to ASIC. However, when the matter requires legal analysis, reasoning and judgment and a determination of whether a matter is reportable due to a contravention of law, and can result in significant civil penalties then it is appropriate in the circumstances that the compliance area wait until its internal or external legal team provides advice in respect to reportability.

In view of the above, we submit that ASIC should remove reference to RG78.80 (b) in RG 78.

B5Q2 Should we include further guidance on what may amount to ‘knowledge’, ‘recklessness’ and ‘reasonable grounds’? If so, please explain what specific guidance would be helpful and why.

Yes we would welcome further practical guidance and case study style examples on these concepts would be useful. Particular scenarios where this would be helpful that have been raised include:

- a. further guidance around the term “reasonable grounds to believe” to help licensees understand the circumstances when this is likely to arise. For instance, could a representative be able to form this view after issuing an FSG knowing he/she had mistakenly used an outdated template, or is it envisaged that an employee or committee with relevant delegated authority would need to make this determination?
- b. Further clarification and examples to define the term “recklessness” would be useful. Whilst the example given at 78.72 is helpful, it would be appreciated if ASIC could provide more examples of circumstances where this is likely to arise. For instance, in determining if there could be reasonable grounds to believe how far does a decision maker need to look before being able form that view?
- c. In relation to the “circumstances known to the licensee” a query has been raised whether this would cover every conceivable data point collected by a licensee even if that information has not been shared with the broader business or entered into the licensee’s relevant risk management system?

B5Q3 Should we include any additional or alternative guidance to help licensees provide reports to ASIC in a timely manner? If so, please give details

See below replies to B6 et seq.

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 Do you have any feedback about the types of information we propose must be included in the prescribed form? If so, please provide details, and identify any issues.

As a general comment, we would observe that the proposed form outlined in Table 8 at 78.88 is a “one size fits all” form and would result in licensees not being able to provide all of the information in every circumstance because of the different nature of reportable situations. For instance, the reporting of an ongoing investigation is unlikely to include information about steps taken around rectification and or client remediation, or information about steps being taken to ensure future compliance. This would result in multiple follow-up communications to ASIC and administrative complexity. In the view of our Members, it is preferable to have different information fields depending on the nature of the reportable situation, with more balanced focus on reporting breaches of the financial adviser as well as the licensee. It is requested that ASIC should also prioritise providing licensees notification of any changes to the Regulatory Portal prior to changes becoming effective.

Please also refer to Annexure 1 which addresses a number of concerns with respect to the Regulatory Portal at paragraphs 11 to 17.

Other specific suggestions raised by our Members are as follows:

- a. Drop down options in the reporting tool, where relevant, and better layout would considerably help with the preparation of the report.
- b. Also, the ability to adjust and update the report online, especially if it is provided prior to deadline, would be beneficial.
- c. Can changes to previous submissions also be recorded as more information is obtained (i.e. as further clarity around the breach and its impact is often obtained as the investigation progresses)?
- d. Where the licensee indicates they are reporting on another licensee it would be preferable if the form allowed less information to be provided as the reporting licensee may not be able to obtain all of the details.
- e. Regarding the nature of one particular reportable situation, it would be helpful if ASIC could provide guidance on which option in the Regulatory Portal to select where an investigation into whether a breach (or likely breach) of a core obligation has occurred and continued for more than 30 days and, within the 30 day lodgement period, further investigations confirmed that there was a significant breach or that there was not a significant breach (or likely significant breach). Neither of these situations should require 2 lodgements.

- f. We suggest ASIC should make available a pro-forma of the prescribed form on their website. Due to the complexity of some breaches, the impacted schemes/products, number of impacted clients and quantum monetary impact will be unknown at the point of breach reporting. The prescribed form should be flexible enough to allow for licensee to either provide this information when available via an update, or allow this to be an estimate.
- g. We note that Table 8 under “Whether and how the reportable situation has been rectified” notes that ASIC expects progress updates on rectification programs, as well as notification that rectification is complete. Does ASIC have guidance on how frequently process reports are to be sent?
- h. Could ASIC consider allowing licensees to extract their breach report data from the Regulatory Portal in a CSV type file format? The guide suggests licensees should maintain a breach register but does not mandate this. For those who do not maintain a register, or for verifying completeness of data held by the licensee and ASIC, a data extract could support this.

B6Q2 Should we include any other information in the prescribed form? If so, please provide details.

Members have noted that the prescribed form needs additional functionality that allows attachments and tables to be submitted to provide context or an easier way to explain the different categories of affected customers. It can be very difficult to communicate exactly what has happened when an example cannot be submitted.

In addition, the Regulatory Portal needs to link to the ASIC messages function more clearly. At present, a message arrives but does not include the ASIC 'Document Number' or 'Reference Number' that connects the message to an investigation/reportable situation. This will be particularly important when the volume increases significantly.

B6Q3 Do you have any concerns about the types of information in the prescribed form and whether this information can be provided within the prescribed 30-day time period? If so, please provide details

With specific reference to the 30-day timeframe, we recommend all questions have the option to record the information was an estimate/approximation, and even not applicable in some instances, at the time of submission. It is not uncommon that it will take more than 30 days to conclude an investigation that establishes the customer impact in full or when it can be fixed.

As a general point, we submit that ASIC should recognise industry concerns that serious penalties can be imposed on licensees if they lodge information in the prescribed form but given the form mandates an answer or the submission cannot be lodged this leaves the licensee in a difficult position where it lodges an estimate in response to a question expressed as an actual number/date.

It would also be useful for ASIC to provide guidance on situations where the licensee is lodging the breach report within the required 30 days but where some of the required information is not yet available. For example, Table 8 includes reference to Future Compliance - You *must describe any steps that have been, or will be, taken to ensure future compliance with the obligation*. Depending on what the licensee may need to do for a particular breach to ensure future compliance it may be hard to provide details in the form within 30 days. Ideas can be

provided but greater time may be required to determine best practice going forward and as greater understanding of the circumstances of the breach is obtained. Table 8 also indicates that the licensee will need to include in the form details of 'Whether and how the reportable situation has been rectified', including when the licensee expects rectification to be complete and how it will be achieved. The licensee may not have this information within 30 days of identifying the breach or potential breach.

See also Annexure 1 at paragraphs 11 to 16.

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 Do you agree with our proposed approach? If not, why not?

As a general comment, guidance would be appreciated however it is noted that licensee compliance systems have a broad operational and risk management scope and it is submitted that it would not be helpful for ASIC to prescribe particular organisational constructs.

B7Q2 Are there any other specific areas that we should consider including in our guidance? If so, please provide details.

Members have expressed a number of concerns regarding the Regulatory Portal set out in the following paragraphs.

As a general point, it is requested that ASIC consult on the functionality, useability and efficiency of the Regulatory Portal design and questions to ensure licensees minimise time required to retrofit what can be a complex factual matrix for breaches and context, into a more rigid and less flexible ASIC breach lodgement Regulatory Portal, where free-field descriptions or nuanced explanations are either not available or highly constrained by the Regulatory Portal functionality. More specifically, in relation to the functionality, useability and efficiency of the Regulatory Portal design we have some additional questions. Namely, will it be modified to:

- a. allow licensees to notify ASIC of a reportable situation without being compelled to enter answers for all questions, or where the only option is binary (e.g. yes or no), allow licensees to answer in a way that is nuanced and not categorically yes or categorically no;
- b. provide licensees with the ability to 'attach' files or a document to a 'transaction'. Presently, there is no mechanism to upload a document or attachment and it can be very difficult to describe in words something that is readily observable in an attachment;
- c. allow the option to provide a draft from the Regulatory Portal for senior executive review. Some licensees currently prepare breach reports internally in a letter format for senior executive review, as the Regulatory Portal is not reader friendly, does not allow table formats or populate the report in draft.
- d. allow updates to a 'transaction' already lodged (e.g. pre-populated) so only new/revised information needs to be entered. This also reduces the risk that the licensee inadvertently enters a different answer to the previous 'transaction' and importantly reduces the need to ask representatives of the licensee to internally re-approve the lodgement of content (including estimates that will appear to be lodged as confirmed facts) that is not relevant to the update sought by ASIC; and
- e. facilitate for messages sent by ASIC and updates to an original breach report to be clearly linked to the matter.

Members have also raised specific concerns specifically regarding publishing information as follows:

- a. Referring to Draft RG78.18 - can ASIC clarify if it will report investigations data that did not/ or has not to date evidenced a reportable situation?
- b. Can ASIC clarify if it will publish the AFSL name and the trading name of the business that has breached?
- c. Can ASIC identify which items in the prescribed form will be used for its publicly available annual reports on breaches?

Finally, it is understood that ASIC is implementing enhancements to the ASIC Regulatory Portal to facilitate breach reporting under the new regime which presumably will be completed by 1 October 2021. On this basis, we submit that the first publication should only cover the period from 1 October 2021. Please could ASIC confirm that this is the case. If not, Members have expressed concern as to the uncertainty of what will the first report contain for the months of July, August and September 2021? In particular, what will ASIC publish from data licensees lodged before the Regulatory Portal enhancements are made (e.g. adding 'estimate' to the binary 'what is the amount... date' options that are prevalent now?) and under the old regime?

Please also see replies to Question B6Q1.

C1 We propose to provide guidance for AFS licensees who are financial advisers and credit licensees who are mortgage brokers. The new obligations require these licensees to notify, investigate and remediate affected clients in certain circumstances. We have set out our proposed guidance in an information sheet: see draft INFO 000 in Attachment 2 to this paper

C1Q1 Do you agree with our proposed approach? If not, why not?

We generally agree with the proposed approach. However, in relation to the concept of a **legally enforceable right to recover loss or damage**, it is noted that it can be very difficult for a licensee to determine if a client has such a right.

C1Q2 Should the guidance we provide on the new obligations be provided in the form of a separate information sheet, or be incorporated into RG 256? Please provide details.

The requirements currently set out in the draft Information Sheet (attachment 2 to the consultation) should preferably be included in RG 256. It is more practical for licensees to have one source of guidance on remediation. The guidance specific to investigating, remediating and notifying clients of misconduct could be a section within RG 256. Also, it would be useful for ASIC to incorporate in the RG 256 how the broader requirements interplay with these requirements.

C2 We propose to give high-level guidance to AFS licensees and credit licensees about the types of information we consider should be included in the notices that must be given to affected clients: see in Actions 1 and 3 of draft INFO 000 in Attachment 2 to this paper.

C2Q1 Do you agree with our proposed approach? If not, why not?

Yes, we agree with ASIC's proposed approach not to provide a standard notification form/template.

C2Q2 Should the form of the notices referred to in Actions 1 and 3 of the information sheet be approved by ASIC? If so, what information, or types of information, should be mandatory, and what should be left to the discretion of the licensee?

The guidance provided by ASIC is sufficient in our view. Licensees should be able to develop their own form and include the information the licensee determines is appropriate and be in a format that works for the licensee. It is good for ASIC to provide the guidance in the Info Sheet, but our view is that it is not necessary to mandate required information.

If you have any queries or wish to discuss any matters raised in this submission, please contact David McGlynn at [REDACTED]

ANNEXURE 1

LIST OF NEW BREACH REPORTING ISSUES TO DISCUSS WITH ASIC

General

1. Clarification on the threshold for significance test. The Exposure Draft (page 10) explains the objective test for significance includes (5)(b) contraventions of civil penalty, or (5)(c) which states that the breach results or is likely to result in loss or damage to clients, or members of schemes. This is a very low threshold and as per examples provided in the Explanatory Memo, only 1 customer impacted (no provision of FSG) can trigger this as significant and the need to report to ASIC. As such this could result in ASIC receiving multiple minor breaches weekly from each AFS Licensee creating a large regulatory burden on financial institutions and on ASIC. Perhaps there could be a materiality or impact threshold, so that, in the FSG example, this could be classified as a “minor or technical breach” and need not be reported. Also, clarification that continuous breaches only need to be reported once.
2. How will ASIC manage breach reports for matters caught by the deeming test which result in trivial, administrative and small matters being frequently reported that do not cause loss or damage to customers. Will ASIC use the regulation making powers to carve these types of matters out.
3. Will there be a material loss and damage monetary threshold for an individual and an aggregate amount of a group of customers.
4. On the other licensee ASIC notification requirements (“dobbing” regime), will there be any protection for the notifying entity, especially any privacy/confidentiality obligations?
5. Clarification on overlap between some of the DDO reporting requirements and breach reporting of other licensee.

Investigations

6. Clarification on the definition of “an investigation” and the “commencement of an investigation”, and if this guidance will be similar to the existing guidance at RG78.28? Would it be appropriate to define this as when the person in charge of Risk & Compliance requests for an investigation to be performed?
7. Clarification of when an “investigation” commences in terms of a licensee “beginning to look into a complaint” (words used in explanatory memo).
8. Clarification on the definition of completion of an investigation. Is an investigation completed when each individual customer impact is known and understood, or when the aggregate portfolio impact is known? Also, clarification whether the quantum of loss/compensation needs to have been determined before an investigation is considered to be completed? It can take a lot longer normally to determine what is each individual customer impact.?

9. How “recklessness” applies in the context of delays in investigation (e.g. investigation does not occur, investigation progress slowly).
10. **ASIC prescribed form:** The EM in connection with investigating and remediating misconduct (EM 12.37 & 12.59) provides guidance regarding the content to include in the notice as well as making reference to forms that may be prescribed by ASIC for notifying clients of an investigation and notifying the outcome of an investigation. Our view is that the EM provides sufficient guidance to assist licensees to develop their own suitable forms and that ASIC should not prescribe any forms.

Questions regarding the ASIC Regulatory Portal

11. Can ASIC agree to changing the functionality of the ASIC Regulatory Portal to allow licensees to notify ASIC of a reportable situation without being compelled to enter answers for all questions? If the new breach reporting laws are reasonably likely to lead to an uplift in the total number of ASIC notifications, due to the need to report ‘investigations’ of reportable situations, can ASIC please accommodate the change to ways of working by allowing many questions to be answered as ‘blank’ or ‘under investigation’. There are now very serious penalties for individuals and licensees for lodging false information with ASIC and the mandatory functionality of the Regulatory Portal puts individuals attempting to do the right thing in an unfairly precarious situation because an accurate number/amount is typically unknown or unavailable at the time of initially notifying ASIC of a new problem. From October 2021 the reporting of investigations is likely to increase the number of reportable situations and these same individuals will be expected to lodge even more estimates in the Regulatory Portal with not ability to select they are not final numbers/dates. Very few questions in the Regulatory Portal allow the person lodging to select an option that reports the answer as an estimate.
12. Can ASIC post a proforma of the Regulatory Portal questions for lodging breaches on the internet in a format that allows licensees to seek internal approval of pre-completed answers prior to lodgement. This will allow a licensee to present a complete set of the answers to the appropriate person(s) to confirm the submission and allow a licensee to meet their record keeping obligations by saving a copy of the answers that were used at the time of lodgement.
13. Can ASIC update the functionality in the ASIC Regulatory Portal so licensees have the ability to ‘attach’ files to a ‘transaction’. Presently, there is no mechanism to lodge examples of the problem that has been identified and it can sometimes be very difficult to describe in words something that is readily observable in an attachment.
14. ASIC presently sends licensees both emails and ‘messages’ from the Regulatory Portal asking for further information but licensees are expected to only answer using a ‘transaction’ via the ASIC Regulatory Portal. Can ASIC please allow a licensee to respond to ASIC using the same method ASIC asked for information because there is no mechanism in the available ‘transactions’ to link the ‘message’ or email to a response. Instead, the available ‘transactions’ require the licensee to **re-enter** the dates, numbers, facts already entered into the Regulatory Portal which are mostly irrelevant to the update sought from ASIC.

15. Can ASIC update the functionality in the ASIC Regulatory Portal so updates to a 'transaction' already lodged are pre-populated so only new/revised information needs to be entered. This will reduce the risk that the licensee inadvertently enters a different answer to the previous 'transaction' and importantly avoids the need to ask representatives of the licensee to internally re-approve the lodgement of content (including estimates that will appear to be lodged as confirmed facts) that is not relevant to the update sought by ASIC.
16. Can ASIC please update the functionality in the Regulatory Portal so 'messages' sent by ASIC are clearly linked to the matter that is relevant to their question. The content of existing messages does not typically include a unique identifier and can be hard to map to the relevant 'transaction'.
17. Could ASIC consider allowing licensees to extract their breach report data from the Regulatory Portal in a CSV type file format? The guide suggests licensees should maintain a breach register but does not mandate this. For those who do not maintain a register, or for verifying completeness of data held by the licensee and ASIC, a data extract could support this.

Breaches involving personal advice

18. Clarification on notification requirements to clients. Please could you confirm our understanding that the customer notification requirements only apply to breaches relating to personal advice?
19. Following on from the above question, if similar customer notification requirements will apply to non-personal advice related breaches, the 10 day customer notification requirements could be challenging to meet, particularly when there is a broad cohort of customers.
20. The refunding of a customer within 30 days after the completion of an investigation could also be challenging, particularly if there are a larger cohort of customers impacted. This is often the case when customer remediation is required for those customers that have ceased to be a customer and our records are no longer current. Also, a refund to be paid within such a tight deadline would be unlikely, especially if there are platforms or multiple intermediaries involved who would need to be engaged to pass on the benefit of the refund.
21. Clarification on what is the threshold for having reasonable grounds to believe that ASIC is already aware of the other licensee breach? Is a confirmation from the other licensee sufficient or must it be publicly known information e.g. relevant ASIC media release?
22. In relation to ASIC processing and publishing information on breaches:
 - a. Will ASIC perform its own due diligence to determine if there are reasonable grounds for the alleged first before publication?
 - b. What information does ASIC intend to publish in relation to breach reporting?