

21 October 2022

Felicity Natoli
Group Senior Manager – Credit & Banking
Financial Services & Wealth
Australian Securities and Investments Commission
Via email: Reportable.Situations.-Feedback@asic.gov.au

Dear Ms Natoli,

Discussion Paper: Reportable Situations Industry Engagement

COBA welcomes the opportunity to contribute to ASIC's program of work to address challenges experienced with the implementation of the reportable situations regime. We applaud ASIC for doing the work to identify challenges and propose potential solutions.

COBA is the industry association for Australia's customer owned banking institutions (mutual banks, credit unions and building societies). Collectively, our sector has \$160 billion in assets and 5 million customers. Customer owned banking institutions account for around two thirds of the total number of domestic Authorised Deposit-taking Institutions (ADIs) and deliver competition and market leading levels of customer satisfaction in the retail banking market. By assets, our entire sector is much smaller than any of the major banks and even our largest member is less than two per cent of the largest major bank.

As the smallest players in the banking market, COBA members are acutely sensitive to compliance cost burdens imposed by regulatory regimes. COBA members report significant increases in costs since the expanded reportable situations regime commenced in October 2021. This is drawing scarce resources away from other priorities in COBA member businesses, such as projects that could be directly benefiting customers. The expanded regime has caused significant increases in the number of breaches that must be reported to ASIC. COBA members are critical of a lack of clarity and insufficient guidance around definitions and also the inflexibility of the reporting portal.

COBA members are particularly frustrated at having to report "paper cuts", i.e. trivial or immaterial matters, and at the complexity of the regime. Detailed comments to ASIC's proposals are outlined below in **Appendix A** and we look forward to working together with ASIC to improve the regime, reduced costs to our members and allow them to maximise the resources they can devote to delivering good outcomes for their customers.

Thank you for the opportunity to provide these comments. If you wish to discuss this submission, please contact Esther Rajadurai, Policy Adviser (erajadurai@coba.asn.au)

Yours sincerely,



MICHAEL LAWRENCE
Chief Executive Officer

Suite 403, Level 4, 151 Castlereagh Street,
Sydney NSW 2000

Suite 4C, 16 National Circuit,
Barton ACT 2600

Appendix A		
Issue 1	F1A.1	Yes, additional guidance would be helpful. ASIC should clarify whether the proposal will only allow grouping of situations that happen within a 30-day window or whether additional situations can be grouped in an existing report whenever new instances of the same group are identified. More information required around whether additional situations can be added if a report is closed.
	F1A.2	No, unlikely to increase regulatory burden.
	F1A.3	Yes. Further guidance on 'single, specific root cause' would be helpful with examples. Clarity preferred around whether reference is to a general 'root cause' category (per lodgement form) or more specifically to a particular set of circumstances.
	F1B.1	Yes. Supplementary guidance may help clarify when 'staff negligence/error' reportable situations should be grouped.
	F1B.2	<p>Guidance from ASIC is needed on what details (and the level of detail) they would expect to see here. Otherwise, there will be inconsistencies in how this is detailed by licensees.</p> <p>A member suggested that a new separate question be created to collect the detail, instead of including within the breach description. The question could then be variable, and only appear where the reporter has selected that they are reporting on more than 1 reportable situation.</p> <p>It is suggested that ASIC clarify in their guidance whether the expectation to report 'staff negligence/error' as the root cause as a last resort (where the licensee has assurance there is no other root cause) only applies to reporting of grouped reportable situations, or whether it also applies to individual reportable situations (i.e. will this expectation also apply in Issue 11).</p> <p>A member also commented that it would provide better insights to clarify why a root-cause was identified rather than why a number of root causes were excluded. Internal systems also require alignment to ASIC root cause categories</p>
	F1B.3	Reporting on why other root causes were discounted would increase regulatory burden.
Issue 2	F2.1	<p>Option 1 is unlikely to provide sufficient clarity given the complexity involved in determining the number of reportable situations.</p> <p>It would also depend on the guidance provided. A member has suggested that the portal could contain the questions that ASIC want answered in the form.</p>
	F2.2	Example scenarios about the most commonly reported to ASIC (E.g. misleading and deceptive conduct, responsible lending, disclosure issues, breaches of efficiently, honestly and fairly etc.) would be helpful. Further, guidance on the permutations themselves would be valuable

		<p>(e.g. noting which permutations in Example 2 are in line or not in line with ASIC expectations), as this guidance could then be applied to a number of different factual scenarios.</p> <p>Further practical guidance requested around how the investigation should be included as a reportable situation to ensure consistency in reporting.</p>
	F2.3	Option 2 would have less regulatory burden as it is a shorter form and easier to complete.
Issue 3	F3.1	Yes, additional guidance would be helpful.
	F3.2	Yes, supplementary guidance will help clarify how to report the number of instances.
	F3.3	<p>Suggest that non-transaction-based scenarios would be useful, such as breaches involving misleading advertising - e.g. incorrect information on a webpage - are instances based on unique views? Overstated interest rate in an email campaign - are instances based on number of emails sent, or number of emails opened?</p> <p>Another member suggested there be guidance around the definition of 'instance'; if customers opened a bonus saver and received misleading information about how to earn the bonus interest yet only 50% of customers actually used the account, would all customers who opened the account be impacted by the incident or only those that used the account; and guidance around how many customers are impacted by an incident where the information on the website is misleading or incorrect (such as an interest rate), or the terms of use on the website are not available due to a broken link and this is the only way customers could access this information. In these situations would you consider everybody who visited the page to be impacted by the incident.</p> <p>Reportable situations involving a joint loan between 2 customers. Single customer with multiple products impacted. It would also be helpful if ASIC provided clarity on how licensees should report if they are not able to determine the exact number of instances (should a worst-case number be provided or best estimate?). An example of this is where misleading information is provided on a webpage. Would ASIC want licensees to report the number of impacted clients as the number of page views while the webpage was incorrect (noting that the bank does not know whether all clients viewed the misleading statement on that webpage or took action based on the information)?</p>
Issue 4	F4.1	<p>Supportive of providing updates when there has been a material change and if there is no change, every 6 months.</p> <p>Suggest ASIC also consider creating specific fields in the portal for updates to allow licensees to provide substantive updates in their own unique field. Also suggest specific fields relating to providing updates on the follow: investigation, assessment, remediation and reconciliation.</p> <p>Suggest portal reports being made available for at least 12 months after closure.</p>

	F4.2	Yes, there would be additional regulatory burden to gather additional updates and submit to ASIC. Supportive of ASIC providing additional details on the level of detail expected to be provided by licensees.
	F4.3	ASIC may wish to consider providing guidance on timeframes for providing updates i.e. once a material change is determined, whether or not the update should be lodged within 30 days. Suggest defining: a material change, a new reportable situation and provide guidance on what the update looks like.
	F4.4	Yes, there would be additional regulatory burden.
Issue 5	F5.1	Supportive of the information outlined in paragraph 44 being used to prompt what information should be included in ASIC reports. It is difficult to list the specific information that should be included given how much the factual circumstances can vary between reports. Another member noted that they found it challenging to have to constantly amend the body of their responses to 'describe the reportable situation' to provide updates on the progression of the investigation and remediation. The ADI suggests as best practice to remove any request for information that may change as the licensees progress the investigation and remediation. Further, supportive of ASIC providing best practice guidance in the form of examples to demonstrate regulator expectations. Setting strict minimum requirements would be more onerous to firms and may not be relevant for all breach types or investigation statuses.
	F5.2	A 'minimum requirement' approach may be less appropriate for some breach types, including: minor breaches with no or minimal customer impact, such as those deemed significant due to a civil penalty provision applying. Providing a long and detailed description may not be warranted in these circumstances. Another example are breaches still undergoing investigation where information known to date may be minimal, and therefore the 'minimum' data cannot be provided as yet. Breaches where remediation/rectification/ compensation field do not adequately cover what has been done to address the issue. Free text also helps to explain drop down fields where additional context or explanation is needed (e.g. if licensees are not able to ascertain the clients impacted with certainty).
	F5.3	A list of minimum requirements could streamline the reporting process as these requirements can be gathered upfront when an issue is first identified. The difficulty will be if licensees are unable to gather all the minimum requirements at the time of reporting. Therefore, Aa 'minimum requirement' could increase the time and effort spent lodging breach reports, which may not be commensurate to the impact and severity of the breach.

Issue 6	F6.1	<p>A list of minimum requirements will possibly streamline the reporting process as these requirements can be gathered upfront when an issue is first identified. The difficulty will be if licensees are unable to gather all the minimum requirements at the time of reporting. Clarity sought around whether it would be ASIC's expectation that this be an ongoing investigation until the minimum requirements are met.</p> <p>In relation to proposal 53 (creating a question asking licensees to “specify the date when it was first identified or discovered that there may be a breach/serious fraud/gross negligence”), a member does have some concerns that this proposal is likely to lead to a change in regulatory burden for licensees as it creates the reporting concept of “discovery” date which is not captured in the legislated breach reporting reforms and would amount to a change in the policy or legislative framework for the already extensive reform regime. This will require further consultation with all stakeholders, including Treasury given this data point was not part of the reform. Welcome more guidance on how ASIC will use this data point and why this new reporting data point is essential and how it sees the “discovery” date interplaying with the “awareness”, “knowledge” and “investigation” concepts under the extensive reform. It would be a regulatory burden outside the ambit of the current reforms to ask licensees to effectively align “discovery” and “investigation” commence dates to demonstrate in reporting to ASIC that there is minimal to no delay between first becoming aware of any potential compliance issue, commencing an investigation and determining whether the potential compliance incident is a reportable situation.</p>
Issue 7	F7.1	<p>Having to provide a name imposes additional regulatory burden on the business to pin-point responsibility on an individual when breaches rarely occur because of a single employee’s conduct and it also raises privacy and procedural fairness questions. If it were to go ahead, the naming of employees and representative should be limited to reportable situations involving serious fraud, gross negligence and breaches involving misconduct.</p> <p>Conduct of an employee of a licensee should be considered the conduct of the licensee themselves in the first instance. If the licensee wishes to report conduct as not being that of the licensee, then it could do so. ASIC has existing powers to seek information if required for an investigation, and can refer to its registers for the names of responsible managers and key persons named against a licence.</p>
Issue 8	F8.1	<p>Proposal is not expected to have an impact on the regulatory burden involved in reporting misleading and deceptive conduct.</p>
	F8.2	<p>Seek guidance from ASIC on how licensees can efficiently report breaches where there is little or no customer loss or impact on market integrity.</p>

		ASIC could consider less fields to be populated in the report where there is little or no customer loss or impact for example, the free text 'breach description' can be less detailed / granular, and commensurate to the impact / severity of the breach.
Issue 9	F9.1	<p>This proposal will significantly increase the regulatory burden involved in lodging a breach report, especially if there is no consideration to the severity of the breach. Whilst a licensee would seek to understand past related or similar breaches to help determine whether the current breach is recurring or systemic, without sophisticated data linkages and systems, this may be difficult to determine with accuracy.</p> <p>A member noted that in the past two years incident reporting and register has moved to a new system solution, therefore older breaches are stored in a separate system and not able to be 'linked' to new incidents recorded. The details within these older breaches are more free-text based, making it difficult to search and classify them e.g. by product/service. In addition, by nature, some breach types would be more likely to be recurring, such as errors in advertising interest rates, which can happen from time to time. Looking back over a period of six-years could provide multiple examples of 'similar' breaches, while offering little to no value in reporting this to ASIC.</p>
	F9.2	A one or two year look back period may be more appropriate in terms of regulatory burden vs benefit derived, and result in higher quality and more accurate and meaningful analysis and responses.
Issue 10	F10.1	<p>Suggest adding that identifying affected clients includes the number of impacted clients and the total financial impact to them (if applicable). Also suggest that the definition include duration of incident.</p> <p>An example or two should be included to provide additional clarity.</p>
Issue 11	F11.1	<p>Any ASIC expectations or guidance on the definitions / usage of these options will require change management within some members' organisations, including staff awareness, training and potentially, system changes (e.g. implementing incident reporting form tool tips / aligning menu options). Consideration should be given to providing for an appropriate transitional period (e.g. 6 months) to allow for implementation of changes.</p> <p>To ensure the guidance is widely read and adopted across the industry, suggest it should be included in RG 78 and also embedded in the ASIC form as an ongoing reminder.</p> <p>Members support embedded guidance that ASIC's preference is that a licensee reports the trigger as a "customer complaint" if that preceded "staff or business unit report".</p>
	F11.2	Members suggest considering situations where customer feedback leads to the identification of a reportable situation. Customer feedback is not captured as a complaint as the customer has not expressed

		<p>dissatisfaction. Clarity on whether this should be put in the 'other' category.</p> <p>Further, unless response inconsistencies are causing difficulties in analysing data by ASIC, responses should be determined by the licensees based on their breach management frameworks.</p>
	F11.3	<p>Additional guidance or definitions would be justified where ASIC has identified that interpretation of a question is commonly inconsistent between licensees and this causes unintended consequences for industry level data analysis.</p> <p>Clarity sought around specifying the last instance of the breach.</p>
	F11.4	Suggestion to include prompts in the portal form.
	F11.5	Will require additional work to implement changes to 'root cause' and 'investigation trigger'. In the short term, it will also require additional training to be rolled out to impacted staff.
Issue 12	F12.1	<p>For some notices the licensee does not have an estimated figure at the time of submitting the form and because the form does not let you proceed without a figure, ASIC will not be getting a clear picture of what is an actual estimate vs what is an arbitrary number used to allow the form to proceed. A more useful approach for ASIC would be to allow the form to proceed with 'to be confirmed' and it can seek further details later from the licensee, or the licensee will update via a supplementary report.</p> <p>ASIC might also consider introducing a free text 'additional client impact comments' field to allow licensees to add any optional comments on the estimated customer impact data, to provide greater clarity to ASIC, such as: where they wish to indicate that this is the maximum cohort potentially impacted, but the real impact is likely lower or where they may wish to provide a range such as minimum and maximum.</p>
	F12.2	Yes, there would be increased burden if ASIC would like a 'worst case' figure of all the potential clients impacted and the financial impact (if applicable) as this would take additional time to gather.
Issue 13	F13.1	Yes, supportive of additional guidance especially around joint accounts. Also seek examples from ASIC.
	F13.2	<p>Yes, information required around misleading information provided on a webpage. Would impacted clients be the number of page views (noting that licensees do not know whether all clients viewed the misleading statement on that webpage)? An additional area of ambiguity is deceased estates. Would the deceased client be included here? Would their beneficiaries? Would their executor?</p> <p>Clarity sought around when a customer who visits a website page which contains misleading information but does not make a financial decision to open a bank account or take out an insurance policy. Would all people who visited the page be considered to be impacted by the incident?</p>
Issue 14	F14.1	Don't perceive any challenges with implementing the proposed change.

Issue 15	F15.1	No challenges perceived as the entity should be able to submit a supplementary report without amending the original report, in cases of errors or withdrawals, and without the need to seek ASIC's permission.
Issue 16		Members agree that relief should be provided regarding high volume, low materiality breaches.
Issue 17		Additional clarification from ASIC would be helpful in this area.
Issue 18		<p>Members would support review of the rolling reporting when there is a requirement to report each 'reportable situation' within 30 days from it arising.</p> <p>A member also stated that the current system is extremely administratively onerous for providing updates as licensees are having to re-input data through the whole form again, rather than being able to update the few relevant details. It would be good if the process could be streamlined so that either the original information is repopulated and it can be confirmed that those details haven't changed, or forms for updates are streamlined to e.g. 2 or 3 questions which allow ADIs to provide only the relevant updated information.</p>
Issue 19		Members feel that providing specific information around the actual preventative measures would be a duplication of what is being provided in rectification. The details will create unnecessary burden and noise in the system as in the case of complex breaches, different approaches are taken by licensees and ASIC can be assured that they have been appropriately dealt with.
Issue 20		Members agree that form design decisions such as greying out fields are restricting the ability of licensees to complete these fields.
Issue 21		Members note that additional questions around remediation and rectification form sections would not add any value and will create unnecessary burden. ASIC's questions around compensation start and end dates are adequate and additional questions would create too much of unnecessary information being reported to ASIC.
Issue 22		Members note that additional product options would be helpful.