Australian Finance Industry Association Limited
ABN 13 000 493 907
L11, 130 Pitt Street Sydney NSW 2000
T: 02 9231 5877
www.afia.asn.au

4 June 2021

Ms Niki De Mel
Strategic Policy Adviser
Strategy Group
Australian Securities and Investments Commission
Level 7, 120 Collins Street
MELBORUNE VIC 3000
Email: Niki.DeMel@asic.gov.au and BR.submissions@asic.gov.au

Dear Ms De Mel

CONSULTATION PAPER 340: BREACH REPORTING AND RELATED OBLIGATIONS

The Australian Finance Industry Association (AFIA) appreciates the opportunity to respond to the Consultation.

As context to this submission, AFIA[1] is a leading advocate for the Australian financial services industry. We support our members to finance Australia's future. We believe that our industry can best support Australia's economy by promoting choice in and access to consumer and business finance, driving competition and innovation in financial services, and supporting greater financial, and therefore social, participation across our community. These principles guide our recommendations in this and other consultations.

AFIA represents over 100 providers of consumer, commercial and wholesale finance across Australia. These banks, finance companies, and fleet and car rental providers, and fintechs provide traditional and more specialised finance to help businesses mobilise working capital, cashflow and investment. They are also at the forefront of financial innovation in consumer finance.

OUR SUBMISSION

For ease of reference, we will refer to the breach reporting requirements introduced for credit and financial services licensees by the *Financial Sector Reform (Hayne Royal Commission Response) Act 2020* (the Act) as 'the breach reporting obligation'.

The breach reporting obligation commences on 1 October 2021, coinciding with the commencement of the design and distribution obligations (DDO) regime, the deferred sales model for add-on insurances,

[1] Australian Finance Industry Association (afia.asn.au)

prohibition on hawking of financial products, and ASIC's reference checking protocol and the commencement of ASIC Regulatory Guide 271: Internal dispute resolution (amongst others).

There are complex interactions between the breach reporting regime and the aforementioned incoming regulatory regimes, as well as foreshadowed future changes including those to the Banking Executive Accountability Regime and the introduction of the Financial Accountability Regime.

In this conflation of complex legal and regulatory change conditions, the financial services industry welcomes clear guidance from ASIC to assist industry with implementation of the breach reporting obligation and ASIC continuing to take a collaborative approach to the process of implementation.

The breach reporting obligation requires licensees to self-report specified matters to ASIC. We note that the final version of the obligations is awaiting confirmation by Treasury, through the release of the Breach Reporting Regulations,[2] in around August 2021. We hope that it can include recommendations by AFIA[3] to exclude from the 'deeming regime' breaches of civil penalty provisions that:

- are documentary or procedural in nature
- contain subjective requirements and can be determined by appropriate external parties (for example responsible lending)
- already provide for a notification to ASIC.

In addition, we understand from our engagement with ASIC that, following the release by Treasury of the Breach Reporting Regulations, ASIC will include a full list of included civil penalty provisions on its website. AFIA and its members fully support this and believe it is important to have this list available at the same time as the publication of Regulatory Guide 78.

Given the cumulative impact and introduction of a number of significant legal and regulatory changes, we put to ASIC that a 'facilitative compliance' approach is necessary to support sensible commencement and transition. The disruption caused by the COVID-19 crisis continues to impact operational priorities and efficiencies – the recent lockdown in Melbourne is yet another example of ongoing uncertainty and operational challenges facing our members. COVID-19 continues to dominate businesses, with bandwidth less capable of focusing on change programs when leadership, resources and programs must focus on looking after employees and customers.

Our recommendations with respect to CP 340 are below.

RECOMMENDATION 1: ENSURE MATTERS THAT ARE 'IN-FLIGHT' PRIOR TO 1 OCTOBER 2021 ARE NOT SUBJECT TO THE BREACH REPORTING OBLIGATION (EVEN IF THOSE MATTERS ARE DETERMINED TO BE REPORTABLE BREACHES AFTER 1 OCTOBER 2021)

The breach reporting obligation commences on 1 October 2021. All licensees currently have risk management processes in place as part of their respective obligations as ACL and AFSL holders. For ACL holders, the breach reporting obligation is a new and requires implementation of a process to capture and review incidents and issues (together referred to as 'Matters').

[2] Financial Sector Reform (Hayne Royal Commission Response – Protecting Consumers (2020)) Regulations 2021: breach reporting
[3] 140421-_SUB_Breach_Reporting_Regulations.pdf (afia.asn.au)

We note that neither the Explanatory Memorandum to the Act nor the Act itself is clear as to whether Matters that arose and were recorded prior to 1 October 2021 and that are under investigation and/or under remediation after 1 October 2021 will need to be reported (if these Matters meet the breach reporting criteria).

AFIA's view and that of our members is that Matters that are identified and logged prior to 1 October 2021 (inflight matters) should be effectively segregated from those that are identified from 1 October 2021 because, if not, it will:

- essentially make the breach reporting obligations retrospective – which we do not believe is the intent of the legislation
- cause confusion and add to the regulatory burden noted above
- allow licensees to implement a clear, efficient and unambiguous breach reporting framework within their organisations
- avoid ASIC being inundated with breach reports for all open incidents and issues on licensees' risk registers (which we also do not think is the expectation or intent).

Therefore, we recommend that akin to the guidance it has given in RG 78.14 and RG 78.15 in relation to AFSL holders, ASIC make clear that Matters that are identified and logged prior to 1 October 2021 and that remain open after the breach reporting obligation commences need not be reported.

RECOMMENDATION 2: SUPPORT INDUSTRY THROUGH IMPLEMENTATION OF THE BREACH REPORTING OBLIGATION AND OTHER REGULATORY FRAMEWORKS

As we note above, with the significant number of intertwining regulatory frameworks commencing in October 2021, it is important that the interplay of these regimes, with the new Breach Reporting Regime is actively considered.

We recommend ASIC be cognisant of this burden and support the industry through the period of implementation by ensuring that its guidance is proportionate and appropriate to the size, business model, and capability of each financial services provider – 'nature, scale and complexity' appropriate.

In addition, we recommend ASIC adopt a 'no enforcement approach' for missed or delayed reporting for the initial commencement phase or commit to working with industry in this period, if it is not able to take a formal no enforcement approach – 'a facilitative compliance' approach.

RECOMMENDATION 3: ENSURE GUIDANCE ON THE SIGNIFICANT BREACHES REGIME IS CLEAR BY PROVIDING FURTHER EXAMPLES AND EXPRESSING ASIC'S APPROACH TO ENFORCEMENT

We note the ASIC Enforcement Review and its intention that there be a more objective 'significant breach' reporting regime so as to allow ASIC to receive greater quality data intelligence.

If Treasury does not adopt AFIA's recommendations in the Breach Reporting Regulations, it will be critical that ASIC provides clarity on the more 'subjective' civil penalty provisions included in the 'deeming regime'.

In particular, it is important that ASIC expresses its expectations for considering whether there has been a reportable breach or not, in situations where there is subjectivity. There are many types of civil penalty provisions where there is some degree of subjectivity about whether a breach has occurred. It will also be important for ASIC to provide specific guidance in relation to ASIC's enforcement policy in relation to

potential breaches of the reporting obligation as it is likely that those subjective 'judgement calls' will be made as to when an entity knew or ought to have known that a reportable situation had arisen and when an 'investigation' had commenced. Given the very wide range of conduct that can give rise to a reportable situation, and the significance of the penalties for a failure to report, there would be a great deal of value in express guidance about the factors that ASIC will consider in deciding whether to take enforcement action.

This will be important to instil confidence in the new breach reporting regime, ensuring consistent, balanced, and evidenced-based reporting that supports the growth of financial businesses as well as competition and innovation across the financial services industry, and conversely, does not create barriers of entry.

To that end, we provide a list of scenarios in Attachment A for ASIC to consider in continuing to develop RG 78.

RECOMMENDATION 4: ENSURE THE REGULATORY PORTAL IS IMPLEMENTED AS SOON AS POSSIBLE

We understand from our conversations with ASIC that the full functionality of the portal will not be available on commencement of the breach reporting obligations and that ASIC will be releasing an information sheet in June 2021 for public consultation, providing practical information on lodging a breach report.

We also note that ASIC will soon be releasing an information sheet for consultation providing practical guidance on the manner and information to be included in a breach report and look forward to engaging with ASIC on this.

Given the cumulative impact of legal and regulatory changes underway in the financial services industry, it will be critical for ASIC, where possible, to dovetail with our members' current processes for compliance and technology changes. Given the projected volume increase in reporting, and lack of a mass reporting option available, the compliance burden and costs involved in implementing the incoming breach reporting regime should not be underestimated.

We again emphasise the potential administrative burden on industry and given the lack of an easy functional portal at the commencement date, we recommend that ASIC should look to adopt a 'facilitative compliance' approach during the initial commencement phase as outlined above.

CLOSING COMMENTS

AFIA recognises the importance of a breach reporting framework in the context of ensuring compliance systems, processes and procedures align with good governance and culture across all financial institutions. It is particularly important in rebuilding trust in the financial services sector.

However, it is important, particularly at this point in the economic recovery, that legislation and regulation is implemented in a proportionate and scalable manner. It is also key that material changes to legal and compliance requirements only occur where there has been demonstrated market failure.

The majority of financial businesses understand the importance of customer centricity, comply with their legal and regulatory obligations, and maintain adequate financial requirements to compensate their customers. Excessive additional compliance obligations and red tape to manage the misconduct of the very few financial businesses that do not maintain good practices and/or behave badly, will contribute to

distracting leadership, resources and programs from immediate priorities as well as impede our economic recovery, and ultimately do greater harm to the wider community.

AFIA represents larger and smaller lenders, ADI and non-ADI lenders. We would be pleased to coordinate a roundtable or further discussion to assist ASIC better understand our feedback and provide practical examples to assist in making sure legal and regulatory changes are made in an appropriate manner.

Should you wish to discuss our submission or require additional information, please contact me or Naveen Ahluwalia, Director of Policy and Regulatory Affairs at naveen@afia.asn.au or 02 9231 5877.

Yours sincerely

Diane Tate
Chief Executive Officer

ATTACHMENT A – EXAMPLES FOR ASIC'S CONSIDERATION IN FURTHER DEVELOPING RG 78

In our engagement with ASIC, it requested examples from our members that would be helpful for it to consider in its continued development of RG 78. Below is a list of examples. We understand that whether a reportable situation arises will be based on actual facts, but we hope the examples provide a general understanding of the types of matters that will trigger considerations as to whether an obligation to report exists.

No	Topic	Examples
1.	**Subjective Obligations – Responsible Lending**	The responsible lending obligations within the National Consumer Credit Protection Act (NCCP) requires licensees to: • make reasonable inquiries about a consumer's financial situation and their requirements and objectives • take reasonable steps to verify a consumer's financial situation, and • make an assessment as to whether the credit contract is 'not unsuitable' for the consumer. RG 209 sets out ASIC's views in relation to these obligations, and it specifically states that a licensee will need to apply its own judgement in determining what is reasonable in the individual circumstances.[4] These obligations are inherently subjective in nature. We also note that the subjective nature of these obligations generates significant volumes of complaints (both internal dispute resolution and to AFCA), particularly in times of economic uncertainty. Our members report that AFCA often determines that a licensee has breached its responsible lending obligations despite the licensee's own view that it has met its responsible lending obligations in extending credit. We have set out our concerns in relation to AFCA's decision making in our response to the Review of AFCA's Terms of Reference, particularly in relation to responsible lending.[5] Therefore, we recommend RG 78 is clear that despite a complaint or allegation that a licensee has breached

[4] Regulatory Guide RG 209 Credit licensing: Responsible lending conduct (asic.gov.au) [RG 208.81]
[5] 010421_SUB_AFCA_Terms_of_Reference.pdf (afia.asn.au)

No	Topic	Examples
		its responsible lending obligations, a complaint to AFCA in itself is not a trigger to report. Further to this, given the subjective nature of certain obligations within the NCCP, we recommend ASIC's guidance states that, even if there is a complaint or an AFCA determination to the contrary, if the licensee has investigated and made a determination that it has not breached its responsible lending obligations, that it is not required to report that breach.
2.	**Subjective Obligations – General Conduct Obligations that are minor or technical in nature**	Section 47 of the NCCP requires credit licensees to comply with general conduct obligations. These conduct obligations require, amongst other things to engage in credit activities efficiently, honestly and fairly, comply with relevant laws, and have adequate arrangements and systems in place to ensure compliance with its obligations as a licensee. As noted above, like the responsible lending obligations, the general conduct obligations are inherently subjective. The concern raised by our members is that one member could interpret say a minor breach of a general conduct obligation, for example servers turning off briefly (which on one reading can be seen as a breach of the obligation to have adequate IT resources in place) as triggering a reporting obligation; however, because it is a subjective call, another could determine it is not reportable. Therefore, we recommend that ASIC provides further guidance around minor and technical issues to avoid receiving a very high volume of incident reporting.
3.	**AFCA – Further Example**	AFCA could make a preliminary finding that a licensee likely did not comply with section 33 of the NCCP because it failed to give to the borrower a periodic statement of account. The licensee disputes this on the basis that notice was given as notification was provided to the borrower that a statement was available for download, even if the customer has not accessed the statement.

No	Topic	Examples
		Can ASIC please clarify if the preliminary views of AFCA (or any other independent arbiter) a is considered determinative of whether a breach or likely breach has occurred. Would ASIC's view change if it was a final determination? To avoid this ambiguity, we reiterate our recommendation that ASIC make clear that a determination by AFCA (or any third-party arbiter) does not in itself trigger a requirement to report.
4.	**Design and Distribution Obligations – Interplay with Breach Reporting Obligations**	We understand from our engagement with ASIC, that ASIC understands the compliance burden on industry and will assist industry in avoiding duplication of reporting. Can ASIC please consider the following scenario, where duplicate reporting is a risk and provide guidance. The following scenario is an interplay between the reporting requirements under the DDO regime and the requirement to report situations about other licensees.[6] DDO is a 'core obligation' for an AFSL holder under section 912D(3) of the Corporations Act and an ACL holder, under section 50A(3)(c) of the NCCP (on the assumption that DDO 'covers conduct relating to credit activities' falling within section 5 of the NCCP definition of 'credit legislation'). Section 994F(4) of the Corporations Act requires distributors to report complaint numbers (including 'nil' reports) to issuers on the timelines set by issuers. This is a civil penalty provision, but it is also a criminal offence, therefore it will be deemed significant and therefore reportable. If a licensed distributor fails to report complaints information to the issuer within 10 business days of the end of the period set by the issuer, a reportable situation will have arisen (under section 912D(1)(a) or

[6] RG 78.20(d)

No	Topic	Examples
		section 50A(1)(a) respectively) and the distributor's obligation to report themselves to ASIC will be triggered. If the licensed issuer has 'reasonable grounds to believe that' (under section 912DAB of the Corporations Act or section 50C of the NCCP respectively): • a licensed distributor has failed to report DDO complaints information when it is required to, and • an individual distributor licensee or employee or director a distributor licensee 'has engaged in conduct that forms part of the reportable situation', and • for an: ▪ AFSL holder – 'the individual provides personal advice to retail clients in relation to relevant financial products' or ▪ ACL holder – 'the individual is a mortgage broker', the issuer's 'dobbing-in' obligation would also be triggered. Further, section 912DAB and section 50C are civil penalty provisions, so any failure by a licensed issuer to report the distributor's breach would also become a reportable situation on the issuer's own account as well. Given the interplay between the DDO reporting obligations and the breach reporting obligations will result in a very high volume of reporting to ASIC, further guidance on a licensee's reporting obligation in relation to this scenario will be welcome.
5.	**Legal Proceedings – Potential Trigger?**	Another example: Say, legal proceedings are commenced against a licensee alleging a breach of the general conduct obligations to engage in credit activities efficiently, honestly and fairly as well as a breach of section 116 of the NCCP in that a preliminary assessment was undertaken improperly.

No	Topic	Examples
		The allegations are rejected by the licensee and a defence is filed. Would ASIC consider reasonable grounds to exist only where a court has determined the matter against the licensee? What if a decision of a lower court is immediately appealed? How is the concept of an investigation to be applied in the above circumstances, where the licensee refutes the allegations entirely?
6.	**Privacy Related Matters**	We note that the general licensee obligations specifically s47(1)(d) of the NCCP (the requirement to comply with the credit legislation, which could include compliance with the Privacy Act) could trigger reportable situations where there is an inadvertent instance of a licensee sending correspondence to the wrong address. These instances could suddenly be reportable to ASIC each time this type of conduct occurs but we do not believe that this is the intention of the breach reporting regime. In our view, privacy related matters are regulated by the Privacy Act, with a trigger within the Act for mandatory data breach reporting to the Office of the Australian Information Commissioner. Please confirm that privacy related matters should therefore be out of scope of the breach reporting obligation.
7.	**Other Reportable Situations**	RG78 would benefit from more guidance on the other reportable situations (such as serious fraud and gross negligence). At present, RG 78 only identifies that these additional reportable situations exist but does not provide any guidance on their scope or application. In particular: • there is a great deal of subjectivity as to when negligence will be 'gross negligence' - some examples would be most helpful • the 'serious fraud' reportable situation is not currently limited to serious fraud in the course of providing the financial services under the AFSL.

No	Topic	Examples
		We assume that this is not intended to capture fraud that is outside of the scope of the AFSL (for example, a representative of a licensee committing fraud in their private affairs or undertaking business activities that are not financial services) Can ASIC please confirm this.
8.	**Third Party Reporting of Other Licensees**	It will be important that ASIC provides further guidance on its expectations in relation to third party reporting of other licensees (for example, the scenario in Example 4). We understand that ASIC's approach is that where a licensee is concerned that another licensee (e.g. mortgage broker) has conducted a breach, they should rely on the facts they have at hand, when making their decision on whether it is a significant breach or not and will need to record it as such. We understand from our engagement with ASIC that ASIC does not expect licensees to have to fact check with the third-party licensee when making a decision. Due to the sensitive nature of the relationships between licensees and their intermediaries, we recommend that ASIC clarify obligations to report on other licensees - particularly whether a licensee would be required to commit resources to investigating if they suspect another licensee has committed a breach. Please also clarify if the approach would differ with respect to an investigation of a licensee's own breach (or likely breach)?