17 May 2017

ASIC Enforcement Review
Financial System Division
The Treasury
Langton Crescent
PARKES ACT 2600

Email: ASICenforcementreview@treasury.gov.au

Attention: Mr Jerome Davidson

Dear Jerome

ASIC Enforcement Review – Position and Consultation Paper 1
Self-reporting of contraventions by financial services and credit licensees

The Australian Financial Markets Association (AFMA) is a member-driven and policy-focused industry body that represents participants in Australia's financial markets and providers of wholesale banking services. AFMA's membership reflects the spectrum of industry participants including banks, stockbrokers, dealers, market makers, market infrastructure providers and treasury corporations.

Almost all of AFMA's members are holders of an Australian Financial Services License (AFSL) and are subject to the breach reporting regime in the Corporations Act.

AFMA would like to provide the following comments in response to the questions in the Position and Consultation Paper.

If you have any queries about this submission please contact me on 02 9776 7997 or tlyons@afma.com.au .

Yours sincerely

Tracey Lyons
Head of Policy

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7907
Email:secretariat@afma.com.au Web: www.afma.com.au

Position and Consultation Paper 1 Questions and AFMA comments

Position 1: The significance test in section 912D of the Corporations Act should be retained but clarified to ensure that the significance of breaches is determined objectively

1.1 Would a requirement to report breaches that a reasonable person would regard as significant be an appropriate trigger for the breach reporting obligation?

1.2 Would such a test reduce ambiguity around the triggering of the obligation to report?

Given the inherent subjectivity, it is not clear that the proposed change to the test will change the way that licensees assess breaches against the reporting obligation, or will reduce the apparent ambiguity around the trigger for reporting. Some of the reasons for this include that:

- A licensee currently makes its own decision measured against the significance criteria, considering the circumstances of the breach in its relevant circumstances – even a reasonable person consideration relies on context. If the test becomes an ordinary licensee test, given the varied nature and scope of licensees, the test will still be dependent on a subjective assessment of what an ordinary licensee is. In which case, the obligation will just end up being considered from the perspective of a reasonable person that looks like the licensee.
- There is an element of subjectivity in the significance criteria itself (which is acknowledged in the paper).
- Most of the obligations in section 912A of the Corporations Act are principles based and rely significantly on a broad subjective assessment of the intent and meaning of these obligations – naturally, in light of any ASIC guidance.
- An objective test in some respects really just facilitates a retrospective consideration of whether someone has met this obligation, rather than necessarily lowering the notification benchmark, which seems to be the goal of any change;
- The nature of the 'reasonable person' may skew the outcome of any test - for example if the 'reasonable person' is a customer they are likely to consider any breach to be significant, whether or not it would meet other criteria used to determine whether that is in fact the case.

Essentially, a regulator wants increased and more timely intelligence to allow it to determine whether regulatory review and/or intervention is necessary. It is not clear that the suggested adjustments to the framework will ultimately deliver this result, or that altering the test from subjective to objective will lead to more consistency in the reporting of matters to ASIC. In saying this, it is agreed that there must be a materiality threshold in the reporting law, otherwise there could be increased inefficiencies in the regulatory system.

There is strong support for increased regulatory guidance. It would be helpful if ASIC could clarify whether the reasonable person test is the sole criteria to be used in determining significance. We believe that significance should be determined by the use of multiple criteria with different weightings – for example, the dollar magnitude of financial loss, the number of customers impacted by the breach, the relative extent to which customers have been prevented from conducting business, whether a law has been broken, and so on.

With reference to paragraph 29 in the Position and Consultation Paper, ASIC must be able to link its guidance to the relevant obligation in the law, and the fact that a breach of the law actually occurs. For instance, there are matters that could result in the disciplining of a licensee's representative that are not a prima facie breach of the relevant law.

Paragraph 29 states that *'..ASIC may specify certain types of breaches that it considers should always be reported'* and then lists eight such potential categories. It would be helpful if ASIC provides a detailed articulation of each of these categories in the regulatory guidance. For instance, Paragraph 29.2 refers a potential requirement to breach report *'matters that could result in the suspension, demotion, termination or resignation..'* of an employee. If interpreted literally, this phrasing (a) infers a requirement to report all employee terminations to ASIC, and (b) could result in a mass of 'breaches' being unnecessarily reported to ASIC – for example, sending inappropriate emails may warrant immediate employee termination for a breach of internal policy, but this would not be a regulatory matter that interferes with the provision of financial services.

Furthermore, it would be helpful if ASIC could provide examples in the guidance of previously reported breaches that are useful to regulators, as this will be more instructive for licensees.

In relation to the examples listed in paragraph 29 of the Paper, it has been noted that:

(a) Paragraph 29.2 is too broad as firms should not be expected to notify regulators in every instance where an employee leaves the firm;
(b) Paragraph 29.4 is too broad and may result in reports of insignificant matters;
(c) Paragraph 29.5 still requires a 'significance filter' as some misleading or deceptive conduct may not be significant; and
(d) Paragraph 29.7 should reflect that penalties change from time to time and it is preferable to provide a list of the relevant provisions to avoid ambiguity.

Position 2: The obligation for licensees to report should expressly include significant breaches or other significant misconduct by an employee or representative

2.1 What would be the implications of this extension of the obligation of licensees to report?

There is concern about the proposal to require reporting of alleged breaches because, as a matter of the fair treatment of representatives, licensees should be hesitant to report individuals without sufficient investigation and evidence of a breach. This risk would be increased if the thresholds for reporting matters are also reduced as proposed in Position 3. At a minimum, to report the conduct of an employee, a licensee should have reasonable grounds for doing so, rather than merely a suspicion of a breach. Representatives who are the subject of an ASIC investigation and/or action, even when not directly implicated, nevertheless can suffer significant duress in the course of ASIC's formal investigatory proceedings. Licensees may also be exposed to a high risk of legal action by employee(s) named in a breach report, including defamation and breaches of employment law.

The meaning of "significant misconduct" is not a sufficiently well-defined term, in light of the statements in the Position Paper that the proposals are aimed at addressing the ambiguity about whether the threshold for the obligation to report is triggered in a given circumstance, and that that significance test should be determined by reference to an objective standard. For example, there may be situations where conduct may be a breach of an internal rule or policy, but not a breach of Australian law.

Similarly, the proposal to report employees who are suspected of not being of good fame and character is a very subjective one, and would bring considerable legal risk to a licensee who alleges such a thing to the regulator without sufficient grounds.

There are considerable sensitivities around licensees establishing the level of certainty needed to report an employee to a regulator, which may lead to the regulator taking significant action against that individual. Licensees have procedural fairness obligations and there are complexities around the burden of proof that must be taken into account in the further development of these reforms.

Position 3: Breach to be reported within 10 business days from the time the obligation to report arises

3.1 Would the threshold for the obligation to report [outlined above] be appropriate?

For the above and other reasons, the proposed threshold is problematic. This would require licensees to lodge a self-report early which may result in excessive noise as incidents may initially appear significant but following further investigation and analysis, might later be identified as, in fact, not a reportable breach.

3.2 Should the threshold extend to broader circumstances such as where a licensee "has information that reasonably suggests" a breach has or may have occurred, as in the United Kingdom?

No, this would be too vague and notifications should be limited to identified breaches. AFMA suggests that providing clearer guidance on what is 'significant' may assist in more timely reporting of significant breaches. The case studies in the Paper where months or years pass before a breach report is submitted should be dealt with in enforcement outcomes rather than changing the standard for reporting to include insignificant and possible breaches.

3.3 Is 10 business days from the time the obligation to report arises an appropriate limit? Or should the period be shorter or longer than 10 days?

Ten business days is not sufficient time to properly and exhaustively determine whether a reportable transgression has occurred. A longer period is preferable to allow licensees to conduct a proper assessment of the circumstances. It will also assist in ensuring sufficient time to obtain accurate and relevant information for inclusion in the self-report. Increasingly, breaches require engagement of multiple areas of the business, IT data extracts and analysis. Providing a small window either requires re-directing resources away from other matters and/or an insufficient period of time to complete a proper review and analysis.

3.4 Would the adoption of such a regime have a cost impact, either positive or negative, for business?

The adoption of such a regime would be a negative cost impact for business. Compliance with the regime will result in increased costs and burden on licensees, including the drains on resources to identify/gather sufficient information to be able to meet the requisite timeframe.

A licensee should have a reasonable amount of time to establish the circumstances of any matter even where there is an early indication that the circumstances may have caused a breach of the relevant law. For example, a licensee may need to seek legal advice to determine the implications of a particular set of circumstances under the Corporations Act, and it may be premature to report the matter to ASIC in the absence of the legal advice. There are significant differences in the evidentiary burden and level of prudence to be applied when considering whether to report matters on the basis of a breach; a likely breach (as opposed to a s912D likely breach); reasonable grounds to suspect a breach; or just suspected breaches.

To improve the efficient of breach reporting, ASIC should introduce a portal to allow licensees to more conveniently report breaches, and add information to existing breach reports. This would improve time-frames and the passage of information between licensees and ASIC.

Position 4: Increase penalties for failure to report as and when required

Generally it has been noted that it is not clear what value will be generated if ASIC has three separate sanction options ie. criminal penalties *and* civil penalties *and* infringement notices. The three separate options may result in confusion, complexity and ambiguity.

4.1 What is the appropriate consequence for a failure to report breaches to ASIC?

If a civil penalty is to be introduced, it is suggested that the courts should have a role in the penalty regime.

Any penalty regime should take into account the severity of the breach and also the rationale for the failure to report ie. if the failure was intentional by the licensee or not.

4.2 Should a failure to report be a criminal offence? Are the current maximum prison term and monetary penalty sufficient deterrents?

A failure to report should only be considered a criminal offence if there was intent and also taking into account the severity of the breach.

If a failure to report were to be a criminal offence, the basis and grounds for reporting must be clear and appropriate. ASIC often has a different expectation of what constitutes a reportable matter (and displays a preference for wanting to know more for market intelligence reasons) than licensees. ASIC should provide improved guidance to the industry, which calls for a measured and pragmatic response rather than a wholly conservative one. If licensees feel compelled to report matters merely because they are concerned about the implications of not reporting (ie. committing a criminal offence) then the significance test risks being distorted, and over-reporting may occur.

Given the seriousness of the potential punishment (ie. incarceration) detailed and specific ASIC guidance is needed, with examples, as to the nature of offences that would warrant a jail term being sought.

Position 5: Introduce a civil penalty regime in addition to the criminal offence for failure to report as and when required

4.3 Should a civil penalty regime be introduced?

Civil penalties should only apply to organisations and not individuals.

Also see response at 4.1 above.

Position 6: Introduce an infringement notice regime for failure to report breaches as and when required

4.4 Should an infringement notice regime be introduced?

An infringement notice regime does not appear to be the most appropriate avenue for addressing a licensee's failure to report. It is not clear what ASIC's regulatory objective in issuing infringement

notices would be and how this is distinct from the regulatory objective in launching civil and/or criminal proceedings.

An infringement notice regime may also act as a disincentive to ASIC's previously stated objective to encourage firms to report early, and may hinder the ability to objectively apply any significance test.

Paragraph 62.3 of the paper refers to a scenario where a firm may be issued an infringement notice even though that firm may not have 'contravened the relevant provision'. Similarly, paragraph 60 refers to the possibility of issuing infringement notices for minor contraventions that do not involve a deliberate failure to report. This implies that a firm could be penalised for failing to report a breach that it was unaware of. It is not clear how such an outcome could be considered fair or reasonable.

Position 7: Encourage a co-operative approach where licensees report breaches, suspected or potential breaches or employee or representative misconduct at the earliest opportunity

4.5 Should the self-reporting regime include incentives such as that [outlined above]? What will be effective to achieve this? What will be the practical implications for ASIC and licensees?

AFMA is generally very supportive of the encouragement of a co-operative approach, irrespective of whether any other changes to the regime proceed.

AFMA supports the proposal to include incentives to encourage reporting and mitigate the risk of not reporting due to fear of legal proceedings. However, the encouragement of early reporting needs to be balanced against the need for licensees to have some level of certainty about the matters being reported. For this reason, there is concern about an obligation to report 'suspected' breaches due to issues such as:

- The difficulty of applying a significance test, and the risk of premature reporting before any significance can be established;
- The likely adoption of a very conservative approach to reporting, resulting in a waste of time and resources for firms and ASIC;
- The delay that can occur between awareness of a potentially reportable breach and the determination that quantifiable criteria have been triggered (such as those described in response to 1.2 above).

In terms of incentives, it has been suggested that ASIC should formally state that it will take self-reporting into account during any enforcement proceedings, and that this is properly reflected in ASIC's dealings with the licensee and in any public statements that are made about enforcement outcomes.

The Corporations Act does not require AFSL holders to maintain a breach register. However, ASIC Regulatory Guide 78 *Breach reporting by AFS licensees,* at RG78.20 says that ASIC considers, in practice, that AFSL holders will need a breach register to ensure that they have adequate arrangements in place to comply with obligations to identify and report all significant breaches (or likely breaches).

Therefore, consideration should be given to requiring the maintenance of breach registers, so that ASIC is in a position to request and interrogate breach registers at any time for the purposes of:

- Assessing the quantity and quality of breach incidents being recorded at first instance (or the paucity of incidents recorded);
- The quality and consistency of breach assessments; and
- Compliance with the notification requirements where a breach has been assessed to be a "significant" breach.

Position 8: Prescribe the required content of reports under section 912D and require them to be delivered electronically

5.1 Is there a need to prescribe the form in which AFS licensees report breaches to ASIC?

AFMA supports a prescribed form for breach reporting. The prescribed form should also include notes to provide further guidance on the type and level of detail to include. The existing Form FS80 *Notification by an AFS licensee of a significant breach of a licensee's obligations* could be used as a starting template. The form should also take account of the fact that a firm may not be able to complete all sections at the time of initial submission, and other information can be added later.

5.2 What impact would this have on AFS licensees?

A prescribed form that can be lodged through an appropriate web portal will assist to standardise the type of information reported and provides licensees with greater certainty as to ASIC's expectations about the level of detail and type of information required.

It is important that the form gives the reporter the opportunity to give a full, accurate and detailed report of the matter. Reporters should not be limited to yes/no or checkbox answers and the form should avoid being geared to any one section of the industry. Licensees should be able to provide sufficient free form information within the report to create as much context as possible.

Position 9: Introduce a self-reporting regime for credit licensees equivalent to the regime for AFS licensees under section 912D of the Corporations Act

6.1 Should the self-reporting regime for credit licensees and AFS licensees be aligned?
6.2 What will be the impact on industry?

It seems reasonable and appropriate to apply the same standards to AFS Licensees and Credit Licensees, especially as a number of entities are both AFS Licensees and Credit Licensees. However, it will be important to avoid duplication and inefficiency for organisations that are dual licensees.

Position 10: Ensure qualified privilege continues to apply to licensees reporting under section 912D

It is essential that qualified privilege continues to apply to licensees reporting under section 912D.

7.1 Should the self-reporting regime for responsible entities be streamlined?

Generally speaking, the greater the level of standardisation in reporting requirements, the greater the level of efficiency that will accrue across the industry. Some AFMA members who are not responsible entities (REs) have related parties who are REs. It is reasonable and appropriate for a streamlined approach to apply, especially given that REs will also be AFS licensees.

Position 11: Remove the additional reporting requirement for responsible entities

7.2 Is it appropriate to remove the separate self-reporting obligation in section 601FC? If so, should the threshold for reporting be incorporated in the factors for assessing significance in section 912D?

Yes it is appropriate to remove the self-reporting obligation in s601FC, and for the threshold for reporting to be incorporated into section 912D. Simplification of the requirements and removal of any potential duplication will help to reduce costs and increase efficiency.

Position 12: Require annual publication by ASIC of breach report data for licensees

8.1 What would be the implications for licensees of a requirement for ASIC to report breach data at the licensee level?

There is considerable concern about this proposal and AFMA urges caution in the further consideration and development of this aspect of the reforms. A number of AFMA members object to the proposal as described in the Paper.
There is potential for a licensee's status to be incorrectly represented, and for licensees with robust compliance frameworks - who may be more likely to identify and self-report matters than others - to be unfairly targeted. There may also be reasons related to the size and complexity of an organisation that mean a larger number of reports may be lodged in a given year.

Mere numbers of breach reports are not an indicator on their own of failings within an organisation, and published data may need to be accompanied by explanatory material in order to fairly represent the circumstances in which the reporting occurred. Even then, the explanation is likely to be lost in the external scrutiny of the number of reports made by a particular firm.

8.2 Should ASIC reporting on breaches at a licensee level be subject to a threshold? If so, what should that threshold be?

For the reasons noted above, AFMA is very cautious about public reporting on breaches at a licensee level. Annual reporting at a firm level may in fact discourage reporting and does not align with the principles about incentives and encouragement of a co-operative approach described elsewhere in the Paper.

Further, as noted above, it may unfairly target licensees with robust compliance frameworks that are more likely to identify and self-report breaches.

It is not clear what value external readers would obtain from data about numbers of breach reports by a particular licensee without the contextual information about those reports.

At best, the breach reporting data could be anonymised and may be more beneficial as an incentive for improved behaviour if it is categorised based on themes that are linked to ASIC's regulatory priorities in financial services – for example xx number of self-reports about client money-related breaches in a year. The categorised data could be supplemented by information about the number of times where ASIC established an actual breach and took some form of disciplinary action, as well as information about the rates of satisfactory remediation by licensees.

AFMA does not dispute that the publication of more specific information that identifies licensees and individuals is appropriate as a deterrent and in the public interest when enforcement action is taken. However ASIC is already armed with the ability to do so when such action is taken, be it in the form of a banning, enforceable undertaking, prosecution or other form of penalty.

8.3 Should annual reports by ASIC on breaches include, in addition to the name of the licensee, the name of the relevant operational unit with the licensee's organisation? Or any other information?

It is not clear what purpose this level of detail would serve, and may cause damage to the licensee's reputation and further deter licensees from reporting. Businesses that adopt a more conservative interpretation in relation to their breach reporting obligations (ie. they lodge proportionately more reports than their peers) may suffer a competitive and reputational disadvantage in having breach reporting data published in the annual report.