26 May 2017

ASIC Enforcement Review

Financial System Division

The Treasury

Langton Crescent

PARKES ACT 2600

Email:

ASICenforcementreview@treasury.gov.au

(In Word and PDF Format)

Dear Colleagues

ASIC Enforcement Review: Position and Consultation Paper 1 (Paper)

Self-reporting of contraventions by financial services and credit licensees

The Financial Services Council (**FSC**) has over 100 members representing Australia's retail and wholesale funds management businesses, superannuation funds, life insurers, financial advisory networks and licensed trustee companies.The industry is responsible for investing more than $2.7 trillion on behalf of 13 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. The FSC promotes best practice for the financial services industry by setting mandatory Standards for its members and providing Guidance Notes to assist in operational efficiency.

Thank you for the opportunity to provide a submission on this topic.

Financial Services Council Ltd
ABN: 82 080 744 163
Level 24, 44 Market Street
Sydney NSW 2000
T: +61 2 9299 3022
F: +61 2 9299 3198
E: info@fsc.org.au
W: fsc.org.au

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

FSC Submission: 26 May 2017

We refer to the Paper and now make the following comments, adopting for convenience, references in the Paper to the Positions taken and questions asked.

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.

Question 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. At the outset, we do note that this is an area where our members' experience and views do differ somewhat but the reasons for those differences are reasonable. We will outline the propositions below. In the result, it may be that the views expressed are not as such that different but each recognise there is a practical need for clarity around the operation of the test;

Comments in the Paper

2. Considered as a matter of high-level principle, such an objective test does initially appear to have some attractions. However, we suggest that a closer examination indicates that the Position adopted in the Paper does present significant difficulties;

3. The Paper suggests that the significance test is subjective, *coupled with some seemingly objective factors to guide licensees in determining whether the objection has been triggered* (paragraph 18). The Paper proposes that more objective test is needed and suggests the following:

> *AFS licensees are required to notify ASIC of matters that a reasonable person would regard as significant having regard to the existing factors set out in subsection 912D(1)(b) of the Act. The flexibility in the existing factors would be maintained with the ability to prescribe additional factors in the regulations* (paragraph 25);

In our view, the current test is **not expressed subjectively** and accordingly, the premise behind this Position with respect is misconceived. The test does not refer to the licensee's own view or state of mind and therefore is not 'subjective'. Instead, the test requires that various criteria relating to the breach in question and the licensee's business be taken into account. This makes the test specific to the particular breach in question and the circumstances of the licensee but this is not 'subjective'. The test is

confined to the circumstances of the particular licensee. This has the practical effect that as between licensees all breaches, irrespective of what they are or deal with are subject to a significance filter, taking into account, amongst other things, the nature of the breach, size complexity and scale of the licensee's business;

4. It seems to us that what the Paper should seek to address are the criteria in s912D (1)(b).[1] At present, those criteria must be assessed in the context **of the particular financial services business,** that is, three of the four criteria in s912D(1)(b) relate to matters that are specific to the particular licensee. These are

(a) the number and frequency of similar previous matters;
(b) the impact of the breach on the licensee's ability to provide the financial services;
(c) the actual or potential financial loss to the licensee itself and;
(d) the extent to which the breach indicates that the licensee's compliance arrangements are inadequate.

Currently, section 912D(1)(b) does not identify any 'per se' breaches requiring notification.

The Paper is concerned that the current test may lead to a failure to report matters that are from a regulatory perspective 'truly' significant or important – in particular, the examples provided refer to situations where the same breach may be considered significant and reportable in smaller organisations, but not in larger organisations (where the breach is assessed having regard to the size of the business);

5. Should that concern be the issue that the Paper is seeking to address, in our view one approach is to amend the factors specified in s912D(1)(b) to deal with both its significance against the specific circumstances of the licensee's business and also the type of conduct or breach that has occurred. This may include setting out clearly in the legislation certain 'per se' significant breaches (although we think that the suggested list in paragraph 29 of the Paper is far too broad as it includes, for example, any breach of Chapter 5C of the Corporations Act). As the Paper itself notes, there is already a power to make regulations to add factors to be considered under s912D(1)(b) (paragraph 25) and this seems a sensible approach. It will provide a degree of certainty for government, regulators and industry and reset reporting expectations in relation to certain categories of breaches. In this context and by way of general observation a number of our members expressed the strong view that the test for breach reporting should be set out in the relevant legislation to the extent possible, rather than being the subject of extensive ASIC guidance;

[1] In this submission unless otherwise indicated, references to sections are references to sections of the *Corporations Act*.

6. In our view, including a 'reasonable person' component to the existing test would not achieve the Paper's stated aims. It would actually increase the level of abstraction and uncertainty when applying the test. This is because licensees would still have to assess each of the factors in s912D(1)(b) as they applied to their business and then imagine a reasonable person also making that assessment.[2] From what perspective is the reasonable person to consider the question? Is it as a reasonable officer of the company, a reasonable regulator, a reasonable institutional investor or a reasonable consumer or 'person on the street'? However, if an objective standard and a reasonable person test were to be included in any amended legislation then that reasonableness test should only apply from the perspective of a reasonable person if they were in the position of the licensee. Further, in terms of review of a licensee's reporting decision, the focus must be on the reasonableness of the licensee's judgment in the then prevailing circumstances, as opposed to what turns out to be the case from an incident in retrospect;

7. Further, the Position would appear to create a significant difference to the breach reporting standards currently applicable under the *Superannuation Industry (Supervision) Act* 1993 (Cth.) and *Regulations* 1994 (**SIS**). Many of our members are dual-regulated, ie reporting to both ASIC and APRA. Creation of distinct reporting regimes is inefficient and burdensome. In this context, we note that the reporting requirements should be harmonised across different regulators, to the extent possible. In this regard there could be value in looking at what ARPA's expectations are in relation to breach reporting by entities it regulates;

8. In this context, it is useful to recall the laudable policy approach adopted when the breach reporting laws for product issuers were aligned under various financial services laws and a single report could be used for both APRA and ASIC: the *Financial Sector Legislation Amendment (Simplifying Regulation and Review) Act 2007* (Cth.). This single approach to regulatory reporting has been of immense importance for a period in the order of a decade for the efficient reporting of regulatory breaches by dual-regulated entities and in red-tape reduction. It seems to us that there is little advantage, and indeed, a number of disadvantages, in not aligning ASIC and APRA breach reporting.

9. We also note that careful consideration also needs to be given to maintaining any relevant symmetry with breach reporting provisions in the

[2] In our respectful opinion, the analogy made in paragraph 26 with continuous disclosure obligations is mistaken as, in that case, the reasonable person test relates to a relatively narrow question of whether the information will have a material effect on the price or value of the entity's securities and not generally as to 'significance'. The UK FCA test is quite different, being anything that the regulator would expect to be notified about. This is really another version of 'significant' or 'material'.

Life Insurance Act 1995 (Cth.) (s132A); the *Insurance Act 1973* (Cth.) (s.38AA) and *the Banking Act 1959* (Cth.); [3]

10. The Position proposed, as we have indicated, may lead to over-reporting and reporting of breaches that may not necessarily be 'significant' especially for large and complex businesses. The current approach has the benefit of distinguishing organisations of different size, nature and complexity. Further, as we have said, the fundamental issue may be better addressed by amendment to the relevant s912D(1)(b) factors or the issue of further Regulations. It might also be useful if ASIC were to provide greater detailed guidance on the interpretation and application of how it perceives the current significance test applying and guidance over what types of breaches should be reported. In particular, it would be useful if specific examples of events which would trigger the breach reporting requirements could be provided;

An objective test?

11. However, as we have said, this is an area where our members' views do differ. Some of our members do support an objective test on the basis of a strengthening of s.912D(1)(b). Thus some of our members do support the introduction of an objective standard into the test for reporting significant breaches having regard to the existing factors listed in s.912D(1)(b). The reasonableness test should apply from the perspective of a reasonable person if they were in the position of the licensee. We emphasise that in terms of review of a licensee's reporting decision, the focus must be on the reasonableness of the licensee's judgement, and after reasonable enquiries, in the then prevailing circumstances, as opposed to what turns out to be the case from an incident in retrospect;

12. On this analysis, the 'significance test' should be retained with clarification to ensure that the significance of breaches is determined objectively. Relevant legislation should provide appropriate clarification of any deemed attributes of the 'reasonable person' and when that person would be taken to regard a breach as significant. Members however, have expressed reservations in relation to the indicative list of types of breaches that ASIC might consider should always be reported (see paragraph 29 of the Paper). The guidance proposed in that paragraph , should:

[3] A point which was made in various submissions to the 2007 *Corporate and Financial Services Regulation Review Proposals Paper* and the *Streamlining Prudential Regulation: Response to 'Rethinking Regulation' Proposals Paper* of 2007 released by The Hon. Peter Dutton, then Minister for Revenue and Assistant Treasurer. This serves to emphasise that any changes in this area should align thresholds for reporting breaches in the Corporations Act and prudential Acts, thereby addressing concerns with inconsistent regulatory requirements, different materiality thresholds and excessive reporting of breaches under the prudential and financial services regulatory regimes.

(a) state that there must be a relevant connection between the conduct to be reported and the services provided under the licence of an Australian financial services licensee (**AFS licensee**);

(b) achieve consistency with the significance test in (amended) s912D. In this regard, we note that the indicative list suggests that for such matters the 'significance test' should not be applied which appears inconsistent with Position 1. If this approach is intentional then, it may create inconsistences and practical issues – e.g. an AFS licensee should not be required to report in relation to an employee's resignation when the resignation has no connection with a reportable matter.

13. One possible approach here is to retain the significance test supplemented by a list of matters that must be reported perhaps monthly or quarterly, irrespective of significance. This removes the potential impact of licensee differences (size, scale, complexity, previous breaches etc) that could otherwise impact on the result. However, it seems to us that matters should not be deemed to be significant. If the concept of a list of" prescribed matters" becomes too unwieldy, then the significance test with appropriate parameters as outlined should be retained. In addition to this information, ASIC would receive its de- identified breach report data on an annual basis. ASIC then could interrogate and analyse all of this data and use its s.912C and other investigation powers should it choose to do so.

In summary, on these approaches, an objective test with more detailed and practical guidance together with continuation of the materiality threshold is supported, particularly given that the provisions relate to entities of different size and scale. To promote the integrity of the industry and deliver a consistent approach there may be some ability to refine these concepts by introducing the concept of "prescribed matters" which need to be reported regardless.

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

14. As we have indicated above, in our view such a test would add further ambiguity and uncertainty to the tests around determining the significance of a breach. It seems to us that this proposed test would not, for the reasons we have mentioned, translate effectively in practice. However, if such a test were to be introduced, then consistent with the alternate view we have mentioned, it does need to be supported by more detailed legislative and regulatory guidance ;

15. As a separate note, in relation to ASIC guidance for breach reporting, our members have indicated support for greater specificity around breach reporting for financial requirements and compensation arrangements;

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

Question 2.1 - What would be the implications of this extension of the licensee's obligation to report (an extension to cover significant breaches or other significant misconduct by employees and representatives)?

Drafting Issues

16. Generally, our members do support the approach, dependent on how the obligation to report is expressed.[4] However; an extension of the obligation in an effective but reasonable way is likely to be complex. We note that the objective of this proposal is to:

> *ensure that ASIC is notified of misconduct or other serious regulatory issues by representatives at the earliest opportunity so that ASIC can, where necessary, investigate and take timely action to remove individuals from the industry in order to protect individuals.*
>
> (Paragraph 35);

However, our members do support a proposal under which there is a specific licensee obligation to report appropriately defined and described relevant significant breaches or other significant misconduct by an individual (including employees, representatives, and Authorised Representatives). Members have noted that such an approach ought to address the anomaly that currently exists where, at law, a breach by an employee representative is deemed a breach by the licensee, but, a breach by an Authorised Representative may not necessarily be a breach by the licensee as well (e.g. if the licensee's compliance framework has operated effectively and efficiently).

17. It is not clear from the Paper whether it is intended that there be a significance test or rather a list of notifiable matters (see paragraph 38). It would be much clearer and better regulation if there was a list of matters that can be objectively ascertained. This is because the licensee is being asked to make decisions and provide notifications about others where those decisions may have grave consequences for those other people;

[4] A different view is noted below.

18. If there were to be a significance test, it would need to involve different considerations from the current s912D(1)(b) because the current criteria would not work when applied to employees or third-party representatives. Further, different criteria also may be needed according to whether the person was an employee (or officer) or a third-party representative (and whether a body corporate or an individual);

19. The Paper suggests that the circumstances allowing ASIC to make banning orders under s920 'should trigger the requirement for the licensee to report' (paragraph 38). This, with respect, is misconceived because a number of these triggers are broad but at the same time technical (for example, *not of good fame and character*) or speculative (*reason to believe that the person is likely to contravene a financial services law*- noting that s920B(1B) extends this to a failure to comply with a duty imposed under the law).;

20. We note that in this context, regulatory guidance ought to be developed as to which acts or omissions amount to "significant misconduct" and "significant breach". The challenges of determining materiality for "significant misconduct" and "significant breach" may be similar to challenges licensees have faced with the term "serious compliance concerns" used in recent ASIC communications. Members also have commented that if the Position were adopted, then ASIC should inform licensees as the outcome of investigations following a serious misconduct report- we note that this may involve specific drafting measures;

21. A related issue, which we believe needs to be addressed, is how the obligation to report breaches applies to a licensee where the breach has been caused by a service provider of the licensee;

Third party service providers

22. (a) Section 912D applies where the licensee itself breaches a relevant obligation. Commonly however, the relevant error is not caused by the licensee itself, but rather by a third party service provider (for example, unit pricing errors or other calculation errors by an administrator). In those circumstances, it may well be unclear whether the licensee itself has breached a relevant obligation, and thus needs to report the error. This is particularly relevant where the third party does not itself hold a licence, or has a licence but does not consider the error to be a significant breach by it, in the context of its overall business;
(b) In 2012, ASIC made some comments in *Report 291: Custodial and depository services in Australia* (**Report 291**) indicating that a breach by a responsible entity's service provider may be reportable by the

responsible entity itself in some circumstances, even if the incident is not reportable by the service provider (see paragraph 42). To the extent to which services provided by a custodian are not 'financial services', any breaches in relation to such services may not be treated as reportable to ASIC by the custodian. However, there may be a breach reportable by the relevant client, if it represents a significant breach or other reportable matter under the client's obligations. For example, a custodian may incorrectly calculate unit prices of a managed fund and in the normal course:

(i) this would not be reportable as a significant breach by the custodian because the calculation of unit prices does not constitute a 'financial service' of the custodian and, in any event, may not be 'significant' in terms of the custodian's business; and

(ii) this would be reportable by the operator of the managed fund to ASIC under section 912D.

(c) However, Report 291 does not address situations where errors by a third party do not result in any relevant breaches by the licensee itself (for example, where the licensee has properly supervised and monitored the third party and has complied with its other statutory obligations);

(d) We appreciate that it is desirable to ensure there is no regulatory gap, and that breaches that occur in these situations are nevertheless brought to ASIC's attention. However, it seems to us that the self-reporting obligation in s912D is not currently drafted in a way that accommodates this outcome, and therefore it creates some uncertainty for licensees in these situations. [5]

Clarification sought

22. We also note to the extent to which it is relevant that in a number of instances, current breach reports necessarily would refer to significant breaches of financial services laws by employees and representatives. However, clarification is required in relation to the concept of "serious misconduct". As you know, the current focus of the reporting regime is around breaches of "financial services law". We note that an example is given in the Paper and paragraph 38 does discuss some of the circumstances where the obligation might be attracted. However, we do have some questions concerning the approach-

(a) Does the concept extend to immoral or unethical conduct (which may not breach a financial services law)?

[5] In this context, we note that the reporting obligation in s601FC(1)(l) is drafted more broadly, by referring to 'any breach of this Act', as opposed to s912D which applies where 'the licensee breaches…'. The current obligation includes notifying when the licensee is likely to breach (although that has a reasonably narrow meaning of the licensee being no longer able to comply (s912D(1A)).

(b) Is the concept intended to have a criminal law meaning?

If the latter is the intention, we question whether procedural fairness and natural justice is to be achieved by reporting a breach (which assumes "guilt") in circumstances where criminal proceedings are in train or contemplated?

23. In addition, it would be useful for our members to understand which employees are contemplated as being covered by the requirement, other than employees of advisers;

24. We also note in this context that consideration will need to be given as to the interaction if any of these measures with other current initiatives and proposals such as reference checking, adviser standards, the ASIC adviser portal and the proposed bank executive accountability regime;

Alternate view

25. As we have said, other members have different views. On this analysis, the extension of the obligation of licensees to report breaches or other significant misconduct by an employee or representative is not supported. The reasoning here is that Australia does not have an individual licensing regime (unlike the United Kingdom) and there is no continuing obligation for employers to track employee's good fame and character. Furthermore, there is currently no guidance in relation to what is considered 'good fame and character' apart from the examples provided in relation to the exercise of ASIC's powers to make banning orders as articulated in s920A(1A). This proposed approach, it is said, appears to be inconsistent with the broader licensing framework.

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

Question 3.1 - Would the threshold for the obligation to report outlined above be appropriate?

Assumption

26. We note in this context that at paragraph 47 of the Paper, the following comments is made:

> *47. The Taskforce adopts, as a preliminary view, that in order to improve certainty and reduce subjectivity in assessing the existence of the obligation to report, the trigger for reporting could be modified so that it is clearly based on an objective assessment of the information available to the AFS licensee. This could be achieved by making the 10 business day timeframe commence from when the AFS*

> *licensee becomes aware or has reason to suspect that a breach has occurred, may have occurred or may occur rather than when the licensee determines that the relevant breach has occurred and is significant.*

We also note that the Paper goes on to indicate that there would be deemed awareness when a licensee is notified by a government agency, an auditor, an industry ombudsman, and

> *50.4. a current or former representative or employee who has provided it to a director, secretary, or senior manager of the licensee or a person authorised by the licensee to receive whistleblower type disclosures.*

27. Having regard to Position 1, we assume that it is still proposed that there be a 'significance' requirement for notification. Accordingly, the ten business day timeframe will commence from when the licensee becomes aware of or has reason to suspect that a **significant** breach has occurred, may have occurred or may occur. Assuming that is the case, there are two fundamental concerns with this proposal;

Concerns with proposal

28. Our first concern is that the proposal requires a licensee to notify ASIC within 10 business days from when the licensee *has reason to suspect* that a significant breach has, may have or may occur. By contrast, s912D currently requires a licensee to notify ASIC within 10 business days from when the licensee *becomes aware* of the relevant breach. This is a material change from the current position and we see very little justification for imposing a reporting obligation based on a licensee's mere suspicion (as opposed to actual awareness) of something that may turn out not to be a breach at all. A licensee should only need to report to ASIC when it has actual knowledge that a breach has occurred. This requires knowledge of both the facts in question and that, as a matter of law, the facts amount to a breach. It is unclear when a licensee will be taken to have a reason to suspect that a breach has occurred? The introduction of such a trigger is likely to create even more uncertainty in the industry. It is already difficult enough under the current test to determine when a person (particularly a corporate entity) has knowledge of something; the need to determine when a person has or should have a suspicion about something would be even more difficult;

29. Moreover, in our view, the proposal does not address the real concern identified in the Paper – that is, evidence of delays by licensees in reporting breaches on the basis that licensees often wait until they have actual knowledge that a breach is significant before they report it to ASIC. The Paper provides case studies to illustrate examples of such delays (paragraph 45). However, in those cases, the existence of a 'reason to

suspect' trigger would not have necessarily meant that the licensees would be required to report the breaches at an earlier point in time – they may still have needed to complete their internal investigations before they could form the view that there was indeed a 'reason to suspect'. We consider the timing aspect of the reporting threshold should involve reporting within 10 days of becoming aware of information that reasonably suggests a reportable breach has occurred. The awareness concept is best supplemented by regulatory guidance that ensures licensees have in place adequate incident management and breach assessment policies in order to support the reporting timeframe in practice

30. (a) This leads to our second concern with the proposal. The proposal does not address the threshold issue that has led to uncertainty in the industry regarding the trigger for calculating the 10 business day notice period. Specifically, section 912D as currently drafted is ambiguous because it is not clear whether a licensee's obligation to notify ASIC is triggered-

(i) when the licensee becomes aware of a breach (or likely breach); or

(ii) when the licensee becomes aware of a breach that is significant (or likely breach that is significant).

Such uncertainty is the reason why (understandably) some licensees do delay reporting breaches to ASIC until they have determined that the breach in question is significant.

(b) Subsection 912D(1B) currently requires the licensee to lodge a written report with ASIC as soon as practicable, and in any case within 10 business days, after becoming aware of 'the breach or likely breach mentioned in subsection (1)'. Subsection (1) refers to 'significant' breaches (para (b)). This suggests that the obligation to report the breach to ASIC arises only when it has been ascertained that a breach or likely breach is 'significant', and the 10 business day period should only begin from that date, not earlier.

(c) However, the drafting is not clear and the alternative interpretation is that the 10 business days begin from the date that the licensee becomes aware of the 'breach' (and not the date that it is determined to be significant). The latter interpretation has been adopted by ASIC but this is in our view not a correct interpretation of the law and is arguably inconsistent with the plain reading of subsection 912D (1B). [6]

[6] In Regulatory Guide 78 (at paras RG [28]-[29]), ASIC says that 'the reporting period starts on the day you became aware of a breach (or likely breach) that you consider could be significant'. The note explains that 'in providing up to 10 days to report a breach, the law allows you to make a genuine attempt to find out what has happened and decide whether the breach is significant. In responding to a breach notification, we will take into account any delays or obfuscation in reporting.' The RG goes on to say that 'because extended processes may defeat the law's intention for ASIC to be informed of significant breaches as soon as practicable, you should not wait until after the following events to send us your report… (a) you have

(d) If current s912D(1B) could be clarified it would help remove inconsistent approaches by licensees to the notification obligations and would be more likely to address the issues identified by the Paper.

One solution would be to amend s912D(1B) so that it reflects ASIC's interpretation of the reporting trigger – that is, a licensee must report a breach (or likely breach) no later than 10 business days after it becomes aware of the breach, unless it has determined within that period that the breach is not significant. If the ASIC interpretation of the 10-day requirement is adopted, it is important that a licensee is not penalised in the situation where the licensee acting reasonably within the initial 10 days determines that the breach is not significant, but subsequent to this, further information gathering reasonably suggests that the breach is significant and the licensee then reports it.

An alternative approach is to make it clear that the 10 business day period only commences when the licensee becomes aware of a 'significant' breach or likely breach, but also imposes on the licensee a positive obligation to take the steps required to make the determination as to 'significance' as promptly as practicable. In our view, any approach which limits licensees' time to assess whether a (significant) breach has occurred to 10 days is not workable and impracticable, for the reasons identified in this paper.

Either of these approaches would, in our view, address the concerns that are identified in the Paper regarding lengthy delays by licensees in reporting breaches to ASIC, and would remove the need to introduce new concepts such as a 'reason to suspect' trigger which would only add to the existing confusion.

Other comments

31. At a very practical level, as we have indicated, the proposal is likely to cause licensees to self-report often and early in point of time which may result in over-reporting. That is, this threshold will significantly increase the likelihood of relatively minor incidents that may not be ultimately significant (because the preliminary view before investigation is that there is reason to suspect that a breach may have occurred) being reported to ASIC. This is likely to be burdensome to both licensees and to ASIC;

32. There does need to be a more objective and reasoned approach in the area; however, the relevant tests need to be clearly articulated and consistent with other reporting regimes (such as SIS). As currently drafted there are ambiguities in the provisions and we have suggested approaches which address these ambiguities. In our view, the proposals are likely to lead to more uncertainty and ambiguity;

---

completed all possible avenues of investigation to satisfy yourself whether or not the breach (or likely breach) is significant…'.

33. In addition to clarifying how the time frame operates in a practical sense, it may also be useful to consider extending the period to say a 30-day period for reporting. The reasoning here is that this may lead to more effective and accurate reporting and appropriate remediation of the relevant issue within a longer time frame and better achieve a good policy outcome;

34. As we have indicated however, some of our members do consider that the proposal does have some merit but requires more detailed refinement and articulation.

Question 3.2 - Should the threshold be extended to wider circumstances, such as where the licensee "has information that reasonably suggests" that a breach has or may have occurred, such as in the United Kingdom?

35. No- consistently with our previous observations, setting a standard against that which "may have occurred" is likely to produce notifications to ASIC that may later be determined to be of minimal or no significance, potentially distracting ASIC's focus and resources from more significant matters. Thus, we do not believe an additional trigger for notification is needed. In any event, we think that deemed awareness is too rigid given the consequences of non-compliance.

Question 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?

36. It certainly should not be shorter, given the time involved in undertaking the necessary internal investigations, obtaining internal legal advice and preparing a sufficiently detailed and properly informed breach report. Thus, in our view, 10 business days should be the minimum period and a longer period is preferable to allow licensees to conduct a proper assessment. It will also assist in ensuring sufficient time to obtain accurate and relevant information for inclusion in the self-report;

37. 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 insufficient time to complete a proper review and analysis. The issue with being required to report prematurely is that the quality of the investigation and

analysis of the issues, and accordingly the information that can be included in the report to ASIC, is at risk of being compromised;

38. If the trigger for reporting is indeed as set out in the Proposal (meaning that a licensee is required to make a determination within 10 business days as to whether it has reason to suspect that a significant breach has, may have or may occur), then 10 business days will often not be sufficient. Based on our members' experience:

    (a) especially in complex situations (for example, in relation to tax calculations or unit pricing errors) it is often difficult, without extensive analysis and expert advice, to establish whether there has been a breach or whether that breach might be significant;

    (b) if it is not possible to obtain sufficient information in the permitted time frame about the potential breach then it is not possible to make an assessment about significance;

    (c) it follows that a licensee will have the dilemma of deciding whether it is better to notify in case there is a breach (and it proves to significant) or wait until there is more information and risk finding, with hindsight, that notification should have been made earlier; and

    (d) if licensees decide to notify 'in case', the notification will only include limited information on the potential breach and a speculative assessment of significance; such a notification will not be very satisfactory or useful from ASIC's perspective.

39. However, if as we have suggested, s912D (1B) is amended to clarify that the 10 business day period commences from the time the licensee becomes aware of a breach (or, alternatively, of a significant breach), then we think the 10 business day period may well be appropriate;

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

40. The adoption of this Position would promote a negative cost impact for business. This may result in a drain on resources to identify and gather sufficient information to be able to meet the requisite timeframe. Moreover, if industry starts to over-report then this will have a negative impact on ASIC's resources as it will be dealing with significantly increased volumes of breach reports, (which may require multiple handling before a complete view is finalised) and many of which may prove to be of minimal significance depending on the threshold for reporting breaches. Further, it is arguable that in the context of significantly increased reporting to ASIC, ASIC will need to be satisfied it has the mechanisms to detect potentially systemic issues in light of the anticipated increased volume of reports.

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

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

41. By way of general observation, we note that there ought to be a degree of proportionality around the consequences: preferably there will be a "tiered" approach to penalties. So, there should be consideration as to why a breach has not been reported. For example, a calculated or reckless breach or disregard of the reporting obligations should be treated differently from, say, a failure to report a breach given a difference of opinion between ASIC and the AFS licensee on the "significance" of the breach involved;

42. Having said that, it seems to us that it is only fair that a breach of 912D should not be an offence unless the current uncertainties in connection with s912D(1B) are resolved (and not compounded). Furthermore, it should not be an offence to fail to report a breach if a licensee believes, in good faith, that there has not been a breach because the tests for both:

> (a) determining whether a breach has occurred (eg whether conduct is misleading, or whether a licensee has acted efficiently, honestly and fairly); and
>
> (b) whether a breach is significant,

are judgement calls on which reasonable minds invariably will differ;

43. One way to address this issue may well be to include a provision that a licensee does not commit an offence if:

> (a) it forms a view, reasonably and in good faith, that there has not been a relevant breach;
>
> (b) it forms a view, reasonably and in good faith, that the breach is not significant; or
>
> (c) it reports a breach within 10 business days of forming a view that a breach was significant, provided that there was no unreasonable delay in forming that view.

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

FSC Submission: 26 May 2017

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

44. As a matter of general principle, our starting position is that it should not be a criminal offence for failure to report a breach. This does appear to be disproportionate to the failure to comply with the legislation. In our view, a criminal penalty regime, if it is to apply, should apply only in the most egregious circumstances of a failure to report and conduct. Further as we have outlined above, the current uncertainties require resolution and if it were proposed to continue to attach criminality to breaches, then certain defences should be available. In essence, it is not clear to us that criminal penalties will have what we assume is the desired impact of increasing accurate and timely reporting levels. Furthermore the interaction with the proposed bank executive accountability regime will need to be considered;

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

Question 4.3 - Should a civil penalty regime be introduced?

45. We think that in principle this would be appropriate: but should be applied on a graduated basis and be subject to the usual safeguards, such as administrative and judicial review.
Any penalty regime should take into account the nature and severity of the underlying breach and also the rationale for the failure to report (whether this was intentional by the licensee or not);

46. Certainly, as a matter of principle, failures to report being a civil penalty would be a better alternative to criminality, possibly with a related offence where 'a licensee intentionally fails to report a [significant] breach of which it has actual knowledge' (paragraph 58). However, any such offence should only apply if the licensee knew that there was an obligation to report the conduct (or was recklessly indifferent as to whether there was such an obligation). It should not apply if the deliberate decision was made with the good faith belief that there was no obligation to report the breach. We note that the civil penalty regime is itself being reviewed by the Taskforce (paragraph 59).

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

FSC Submission: 26 May 2017

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

Question 4.4 - Should an infringement notice regime be introduced?

47. It is not clear to us that such a regime would be the most appropriate avenue for addressing a licensee's failure to report. In our view, infringement notice regimes are bad policy and structurally unfair because they put the regulator in the position of both prosecutor and adjudicator. We note that infringement notice regimes are also under review by the Taskforce (paragraph 64);

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

Question 4.5 - Should the self-reporting regime include incentives such as those outlined above? What will be effective to achieve this? What will be the practical outcome for ASIC and licensees?

48. The Paper discusses the possible inclusion of *provisions that encourage a collaborative approach between the regulated and regulator and encourage licensees to report events and information to the regulator at the earliest opportunity, even where proper investigation of the circumstances may take some time and resources of the licensee.* (Paragraph 65)

49. We do note however that attempts to encourage a co-operative approach are likely to be unsuccessful while the regime provides for criminal offences. The Paper suggests that there be 'a formal provision expressly allowing ASIC to decide not to take action in respect of licensees when they self-report and certain additional requirements are satisfied' (paragraph 67). But ASIC can, and does, do this now. However, it may assist if guidance were given as to factors which ASIC should take into account in deciding whether to take action. These factors could include:

(a) whether the breach was dishonest;

(b) whether any losses were caused by the breach (and, if so, their quantum);

(c) what action was taken by the licensee to remedy the breach;

(d) what action has been taken by the licensee to prevent future, similar breaches;

(e) whether the breach is indicative of systemic issues in the licensee;

(f) when the breach was reported; and

(g) whether the licensee has co-operated with ASIC.

The Paper suggests a provision allowing ASIC to decide 'to take no administrative or civil action against the licensee if the licensee cooperates with ASIC and addresses the matters to ASIC's satisfaction' (paragraph 68). Again this can happen now and can be given a level of formality (and precision) through enforceable undertakings.

As a cautionary note however, we do express some reservations with this incentives approach that it may result in the regulator aiming to achieve compensation outcomes that extend beyond the loss to clients (if any) as result of the breach. In this respect, we query whether the option described in paragraph 68 should be prescribed at all - we would assume that following these steps should already provide the licensee with a degree of comfort that enforcement action is unlikely to ensue. ;

50. In summary then, provided elements of criminality were removed and there were appropriate design measures and safeguards to address concerns such as those noted above, we would support this approach as a matter of general principle. The relevant mechanisms should encourage positive behaviour, such as timely self-reporting (i.e. a "carrot"), and then build in penalties for failing to comply (i.e. a "stick") then this could assist in "nudging" the desired behaviours. Another "carrot" would be that, particularly if the threshold for reporting breaches is lowered to a standard such as suspicion a breach may have occurred, when a licensee reports early or on time, then ASIC should effectively be precluded from acting on the report until after a certain timeframe. Importantly, this should be an objective, clearly established regime and not entirely reliant upon ASIC's discretion. It needs to be carefully considered, contain appropriate safeguards and should be the subject of further and detailed consultation with industry;

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

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

51. In broad terms, we do not have any objection, as such, to a form for breach reporting being prescribed. However, the form should be fit for purpose and cover a range of scenarios where the reporting

obligation is triggered. We are not certain whether this is possible to achieve. Currently, the recommended form (Form FS80) is not fit for purpose, as it is very narrow and prescriptive and contemplates that there has been a breach, rather than a likely breach. It has been structured to allow for information to be collected and used efficiently and for data analytics. ASIC already provides guidance on matters that should be covered in a notification (Regulatory Guide 78 – RG78.23 to 78.26). For completeness, we do note that reporting to APRA is electronic and is tightly prescriptive (at least for superannuation trustees). Thus, a prescribed form of ASIC reporting would not assist dual-regulated superannuation trustees under current arrangements. However, in this regard, it might be useful if ASIC and industry were to consult to develop a prescribed or recommended form in which licensees report breaches to ASIC. Through a consultative approach they can ensure that the prescribed form is workable, sufficiently flexible, and effective – this approach would replicate previous successful consultations on data collection (e.g. the consultation on the lapse reporting initiative, and the consultation on the public reporting of claims handling data).;

Question 5.2 - What impact would this have on AFS licensees?

52. This will depend on the final version of the form but we suspect this will be minimal, assuming there is sufficient flexibility in relation to the form (as contemplated by the Paper - paragraph 76);

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

53. No detailed response as such as "credit" is outside the FSC's constituency. However, by way of general observation, as we have indicated, any changes to the reporting regime under section 912D should be made having regard to other breach reporting obligations, in particular, those of APRA regulated entities, such as those governed by SIS and the other legislative items, as we have mentioned. The same applies to any new reporting regime under the *National Consumer Credit Protection Act 2009* (Cth). We also note in this context that the interaction between and overlap of reporting obligations of entities regulated under both the Chapter 7 of the Corporations Act and APRA should be reviewed: while s912D(1C) is an attempt to avoid duplication and repetition, in practice this is neither clear nor simple;

We also think the current review presents an opportunity to revisit the legislation that is listed in regulation 7.6.02A of the Corporations Regulations (for the purposes of s912D(1)(a)(iii) of the Corporations Act), in order to determine whether it is appropriate for those items of legislation to be covered by the s912D breach reporting regime. For example, SIS is mentioned in regulation 7.6.02A, but in our view the SIS Act does not govern 'conduct relating to the provision of financial services', referred to in paragraph (d) of the definition of 'financial services law' in section 761A (which is in turn referred to in s912D(1)(a)(iii)). It is therefore unclear to us whether a breach of the SIS Act would ever need to be reported to ASIC (as well as APRA) under section 912D.

54. We believe the review also presents an opportunity to consider the potential application here of s38A SIS. This provides that a breach of certain sections of the Corporations Act are taken as breaches of SIS, and therefore must be reported to APRA (as well as being reported to ASIC): refer to the list in paras (b) & (c) of "regulatory provision" in s.38A SIS. Other than the insider trading provision (s.1043A), these are disclosure items which are clearly in ASIC's bailiwick. It is not clear to us that APRA really needs to be made aware of these matters by way of breach reporting. One of our members has indicated that the usual APRA response is that it notes the report and leaves the matter to ASIC (as it must under the allocation of responsibilities between the regulators). It may well be that these provisions are an outcome of the 2002 FSR reforms when the SIS Regs disclosure provisions were relocated to the Corporations Regulations. For matters which are of enhanced significance such as a PDS stop order or a false or misleading statement, presumably APRA would be advised in any event pursuant to the ASIC-APRA MoU on the exchange of information. Our view is that *regulatory provision* in s.38A SIS should be limited to laws for which APRA is the lead regulator, and the Regulators' MOUs are used for those occasions where another regulator needs to know about a trustee's other conduct. That is, there should not be reporting to APRA under para (a) of s.38A of a breach of a provision of SIS where APRA is not the Regulator under s.6 SIS. At the very least, we suggest that paragraphs (b) & (c) of s.38A be removed.

Question 6.1 - Should the self-reporting regime for AFS licensees and credit licensees be aligned?

55. Although this is not as such an area within the "constituency" of the FSC, we agree for the sake of legislative uniformity and good policy, that there is merit in the proposal.

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

FSC Submission: 26 May 2017

Question 6.2 - What will be the impact on industry?

56. There may well be significantly increased compliance costs for smaller operators, especially those who do not already hold an AFS licence and so who are not currently required to comply with the AFS licensee breach reporting regime.

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

57. We agree with the comments concerning retention of privilege.

Position 11: Remove the additional reporting requirement for responsible entities

Question 7.1 - Should the self-reporting regime for REs be streamlined?

58. Yes-we agree that a streamlined and consistent breach reporting process should apply for REs. One of our members has noted that a matter that gives rise to a reporting obligation under section 601FC(1)(l) will invariably also trigger a notification under s912D (paragraph 100) and a 'combined' notification is usually given. That said, the member has indicated that it would accept the addition of a new paragraph to s912D(1)(b) to specifically refer to material adverse effect on members' interests (paragraph 102).For completeness, we do note that given s.912D(1)(b) already includes the criterion of actual or potential financial loss to clients, the addition of the s.610FC(1)(l) threshold may be redundant. This does emphasise that careful consideration should be given to any drafting in this context to make sure that all provisions "mesh" and work effectively.

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

59. Yes: however, on one view, it is preferable that the threshold for reporting in 601FC should be incorporated into accompanying updated

ASIC guidance on breach reporting, rather than incorporated into 912D itself;

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

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

60. As a broad proposition, we do not support the concept of ASIC reporting breach data at a licensee level. Regarding this proposal the Paper says:

> *The Taskforce's initial view is that reporting should be confined to significant breaches, and should be at the licensee level, but could extent to identifying the operational area of the licensee's organisation in which the breach occurred. This would assist in enabling industry and consumers to identify areas where significant numbers of breaches are occurring and provide licensees with an incentive to improve their compliance.*
>
> (Paragraph 106)

61. The claimed beneficial results of this increased disclosure are speculative and may have unintended consequences (for example, entities actually limiting notifications to avoid publication). Also, it would require ASIC to allocate resources to the additional reporting for no clear benefit. Another consequence is that the proposal could incorrectly represent the licensee's status and unfairly target licensees with robust compliance frameworks, who are more likely to identify and self-report matters than others who do not have such frameworks. Also, the proposal does not appear to take into account the size and complexity of an organisation;

62. In relation to breach reporting at a licensee level, we also make the following general observations. We appreciate that views in this area may differ and other organisations may have different views. We do not know precisely the number of licensees in the financial services industry. However, this is unlikely to be a small or even readily manageable list. Another alternative aligned to increased transparency could be for better aggregation into types and size of licensees or across industries and if necessary refined according to type of regulatory breach. This approach may present a compromise solution. We do question the level of detail required for transparency purposes. In the result, ASIC will have that detailed information and already has flexibility as to what announcements it makes at a public level either when an investigation starts or when it is completed. ASIC often includes this data in its annual reporting. This also brings into question what

additional regulatory purpose is served by a granular approach to publication. It could also support the very name and shame regime that is being considered in other fora. Further, different types or magnitudes of breaches may have no consumer loss or detriment. However, how these are explained and detailed through any public reporting requires more detailed consideration and consultation. In this context, we also question what the attitude of APRA would be to this level of reporting when prudential related issues are involved. This in itself requires further consideration.

63. However, if breach-reporting data were to be published, which we oppose as a starting proposition for the reasons given, then it should be anonymised: it should not name individual licensees. In addition, there may be benefit in categorising reports based on themes and where ASIC establishes a breach and takes appropriate action. Summary data can be prepared based on the information that is made public.
Unfortunately, experience shows that the "naming and shaming" of particular individuals or organisations has the propensity to lead to often ill-informed and unbalanced media comment and scrutiny.

If it **is** decided that it is appropriate to name individual licensees, then such references should only relate to overall number of breaches reported. Any granular detail about the nature of the breaches should be anonymised, to show industry themes, client impacts and like matters.

In our view, any reports of "suspected matters" should be excluded from the regime, as these matters have not been finally determined. Individuals subject to banning, criminal conviction or civil penalties are currently published in ASIC's six monthly enforcement reporting. ASIC already has the ability to determine the frequency of this reporting. Additional reporting or naming of individuals is not appropriate and should remain restricted to those subject to findings of fact regarding misconduct.

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

64. If ASIC does report breaches on a licensee level, contrary to our submissions, then it should be subject to a materiality threshold, for example where the breach, once investigated, has resulted in a penalty being imposed or where there has been significant client impact. This is particularly so if the threshold for reporting breaches is lowered, and issues are reported early to ASIC but are eventually found to be of minimal significance or possibly not even a breach. Reporting in such circumstances would have the effect of unfairly penalising licensees and may act as a disincentive to early reporting. We do emphasise that If there is to be a threshold, it should not be frequency of reported breaches because that may provide a disincentive to report;

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

FSC Submission: 26 May 2017

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

65. No, we perceive any value in naming the relevant operational unit. The more detailed the information to be included, the greater the risk that licensees will want to avoid reporting. In addition, in our view, organisations which have adopted a more conservative interpretation may suffer from competitive and reputational disadvantage in having breach reporting data published in the annual report.

Should you have any questions, please contact the writer on 02-9299 3022.

Yours Faithfully

Paul Callaghan
General Counsel