FINANCIAL PLANNING
ASSOCIATION of AUSTRALIA

12 March 2017

Manager
Corporations and Schemes Unit
Financial System Division
The Treasury
Langton Crescent
PARKES ACT 2600

Dear Sir

Self-Reporting of contraventions by financial services and credit licensees

The Financial Planning Association of Australia (FPA) welcomes the opportunity to provide comments to the ASIC Enforcement Review Taskforce on Position and Consultation Paper 1.

The FPA supports a breach reporting system that aims to improve the quality of financial advice and services for consumers.

We would welcome the opportunity to discuss the matters raised in our submission with you further. If you have any queries, please do not hesitate to contact me on 02 9220 4500 or heather.mcevoy@fpa.com.au.

Yours sincerely

Heather McEvoy
Policy Manager
Financial Planning Association of Australia[1]

[1] The Financial Planning Association (FPA) has more than 12,000 members and affiliates of whom 10,000 are practising financial planners and 5,600 CFP professionals. The FPA has taken a leadership role in the financial planning profession in Australia and globally:

- Our first "policy pillar" is to act in the public interest at all times.
- In 2009 we announced a remuneration policy banning all commissions and conflicted remuneration on investments and super for our members – years ahead of FOFA.
- An independent conduct review panel, Chaired by Mark Vincent, deals with investigations and complaints against our members for breaches of our professional rules.
- The first financial planning professional body in the world to have a full suite of professional regulations incorporating a set of ethical principles, practice standards and professional conduct rules required of professional financial planning practices. This is being exported to 24 member countries and 150,000 CFP practitioners of the FPSB.
- We have built a curriculum with 17 Australian Universities for degrees in financial planning. Since 1st July 2013 all new members of the FPA have been required to hold, as a minimum, an approved undergraduate degree.
- CFP certification is the pre-eminent certification in financial planning globally. The educational requirements and standards to attain CFP standing are equal to other professional designations, eg CPA Australia.
- We are recognised as a professional body by the Tax Practitioners Board

FINANCIAL PLANNING
ASSOCIATION *of* AUSTRALIA

ASIC ENFORCEMENT REVIEW
Self-Reporting of contraventions by financial services and credit licensees

FPA submission to

Treasury

12 March 2017

Financial Planning Association of Australia
GPO Box 4285 Sydney NSW 2001
fpa@fpa.com.au
www.fpa.com.au
t 1300 337 301
ABN 62 054 174 453

Introduction

The Regulator plays a fundamental role in ensuring the confidence and protection of consumers which is paramount to the effective and sustainable operation of Australia's financial service sector.

While ASIC awareness of potential breaches may assist in facilitating Regulator action in response to significant incidences, a bigger stick and clearer breach reporting requirements will not necessarily improve the quality of financial advice for consumers, nor is there any evidence it prevents financial advice failure.

Improvements in the breach reporting system must be consumer focused, and balance the need to enhance transparency, increase ASIC's ability to be made aware of breaches in a timely fashion to protect consumers, support investigative due process, and ensure the finite resources of licensees and the Regulator are spent on issues at risk of causing significant consumer detriment.

The FPA provides comments on Proposed Positions that relate to licensees who provide financial advice only. We have not provided comments on matters related to consumer credit licensees.

Key concerns

Objectives

As indicated in the Minister's media release:

> *"The proposals outlined in this paper are aimed at improving transparency and accountability in the financial services sector by broadening and strengthening the obligations on licensees to make timely reports to ASIC about misconduct or suspected misconduct that they become aware of"*[2]

However, the Consultation Paper does not set clear objectives about the purpose for ASIC's breach reporting regime. Nor does it acknowledge that risk management practices and systems are not perfect. Systems will fail at some time and to some extent. Understanding ASIC's level of tolerance for such systems is vital.

Government and consumers have an expectation that every breach will be detected and reported to ASIC. However, this creates a significant risk that resources become devoted to tick-a-box compliance rather than a culture focused on the end consumer – a culture that is driven by ensuring optimum systems and processes are in place to drive improvements in the quality of the financial advice and services provided to consumers.

As indicated in ASIC Report 515, consumer outcomes over the past ten years, coupled with the increase in compliance based regulation since the introduction of the Financial Services Reform (FSR) and other more recent measures, demonstrate that a focus on compliance has not delivered improvements in the quality of financial advice and services for consumers.

There are many competing interests and issues in breach reporting. While Government is concerned about public perception of looking after the best interests of Australians with ASIC as its enforcer, consumers are more focused on justice. There must be clearly established goals and objectives that

[2] Media release - ASIC enforcement review consults on breach reporting, Minister for Revenue and Financial Services, the Hon Kelly O'Dwyer MP, 11 April 2017

elevate the ASIC breach reporting system above these issues, to ensure there is focus on a primary driver for breach reporting – this should be improving the quality of advice and services for consumers, not for ASIC to increase its number of prosecutions.

Recommendation:

Undertake appropriate consultation to establish clear goals and objectives for the ASIC breach reporting system, that focus on improving the quality of financial advice and services for consumers.

Industry Funding Model for ASIC

Much of the commentary and proposals in the Consultation Paper seem to focus on large licensee behaviour and reporting. As discussed in the Consultation Paper, given the current application of the significance test by large licensees, there is the potential that any changes to the breach reporting requirements will increase self-reporting particularly from the large licensee market segment.

The ASIC Supervisory Cost Recovery Levy Bill 2017 currently before Parliament and the accompanying draft Regulations indicate that ASIC surveillance and enforcement activity will be recovered via an industry levy applied at a sub-sector level – that is the cost will be shared across all licensees regardless of scale, or the nature or complexity of the business.

The Government's cost recovery approach to regulation has a significant impact particularly on small business, market competition, and creates flow on effects for consumers.

While monitoring and enforcement is paramount to an effective regulatory system, it is concerning that the breach reporting Consultation Paper is silent on the budget impact the proposals are bound to have for ASIC, be it through additional workload, resource requirements, or the need for enhance technologies.

For example, will the resulting additional activity be added in the surveillance and enforcement buckets with the cost shared across all sub-sector licensees, even though an increase in self-reporting is anticipated from large licensees in particular; similarly, how will the proposed cooperative approach to breach reporting will be funded, including potential additional ASIC resources to approve and oversee breach investigation programs?

Given the stated expectation of the changes leading to an increase of breach reporting and the Taskforce's proposed sanctions regime, it is important that penalties incurred by licensees and individuals from the resulting ASIC action, help fund the Regulator.

We also question whether ASIC has the capacity to implement the Taskforce's proposals, particularly in receiving the likely increased volume of breach reports, and the flow on effects to the levy with the need to increase capacity.

Recommendations:

In developing its final recommendations, the Taskforce should consider the flow on consequences to the ASIC funding model.

Penalties for breaches of laws administered by ASIC should be allocated specifically to ASIC (to contribute to ASIC funding) and not allocated to Consolidated Revenue.

FASEA

The *Corporations Amendment (Professional Standards of Financial Advisers) Bill 2016 set new education and professional standards financial advice providers. This* included the establishment of an independent standards setting body, the Financial Adviser Standards and Ethics Authority (FASEA).

The FASEA will be responsible for governing the conduct of professionals in the financial advice sector, by setting mandatory educational and training requirements, developing and setting an industry exam, and creating a Code of Ethics that all advisers will be required to adhere to.[3]

The Code of Ethics will commence on 1 January 2020, with all advisers being required to adhere to the code from that day forward.

The reporting requirements for the new Code of Ethics are yet to be set. Monitoring will be done by ASIC approved Code of Ethics monitoring schemes. To ensure the effectiveness of the Code and the efficiencies of reporting systems, there must be an integrated approach between ASIC self-reporting requirements for the Acts it administers and FASEA's Code monitoring arrangements.

Recommendation:

ASIC self-reporting requirements must be integrated with the Code of Ethics monitoring arrangements under the education standards and ethics legislation and FASEA.

Co-regulation - Regulators and professional bodies working together

The FPA suggest there is a fundamental need to recognise the role professional bodies can play in assisting ASIC to achieve its mandate under the ASIC Act, in order to improve overall consumer protection.

Industry specific obligations set and enforced by professional bodies, greatly complement the requirements of Corporations Law regulated by ASIC. Corporations Law requirements are over-arching and do not speak to the specific roles, services, and interactions provided to consumers by the various industries within the Australian financial services sector. Professional obligations are industry specific and provide a vital contribution to protecting consumers.

The FPA's professional obligations and activity are focused on the part of the financial services sector to which the FPA belongs, that is the financial planning profession. Our obligations and activity are specifically designed to govern the conduct of our members in the provision of financial planning services to consumers, and in turn the needs of the consumers seeking the services of our members. Therefore, they have a significant impact on the conduct of our members and the consumers they serve.

Co-regulation based on a collaborative two-way partnership between the Regulator and professional bodies is a cost-effective way to enhance consumer protection.

[3] Media release - *Financial Adviser Standards and Ethics Authority appointments*, Minister for Revenue and Financial Services, the Hon Kelly O'Dwyer MP, 10 April 2017

Currently ASIC's work with professional bodies is based on limited ad hoc issues. Formal arrangements should be established between ASIC and professional bodies, through a Memorandum of Understanding (MOU), that ensures a focused and ongoing partnership that enables parties to work openly together to deliver a stronger and more effective regulatory environment for all stakeholders.

The current system does not always allow or facilitate such arrangements creating significant inefficiencies and duplication of costs to the detriment of consumers, industry and government.

For example, recently ASIC and the FPA simultaneously banned a financial planner, Darren Tindall. This means, the FPA and ASIC conducted the same investigations and came to the same conclusions at the same time. This highlights the unnecessary duplication of effort and resources that could be avoided were a collaborative approach permitted.

This collaborative approach must include accepting and acting on breach reporting information.

The TPB has set a precedent for a co-regulatory approach as they proactively share with approved professional bodies, information regarding their investigations and findings against breaches of the relevant laws by regulated entities.

Recommendations:

- The Government launch an Australian Law Reform Commission inquiry to establish co-regulatory professional accountability systems, including supporting legislation placing obligations on ASIC and Licensees to co-operate with professional bodies.
- Impose an obligation on licensees to report breaches of professional obligations by individuals to professional associations.
- To avoid unwarranted damage to professional reputation of the individual, there should be a (high) threshold for reporting individual conduct directly to ASIC, and a lesser threshold for reporting individual conduct to professional association.
- ASIC should only be expected to act against an individual where the higher threshold is breached, and should be empowered to remit a matter for professional association discipline in the appropriate case.
- ASIC should be required to information share with professional bodies by:
    - Amending Regulation 8AA of the ASIC Regulations to include other financial services professional bodies, including the Financial Planning Association, and permit collaborative and confidential information sharing between ASIC and professional bodies to enhance consumer protection.
    - Permitting the establishment of Memorandum of Understandings between ASIC and professional bodies that facilitates and permits a more collaborative and cooperative two-way working relationship, or co-regulatory partnership.

Professional indemnity insurance

ASIC's Regulatory Guide RG126 sets out how the Regulator administers the compensation requirements under s912B of the *Corporations Act 2001.*

Corporations Regulations 2001 (Corporations Regulations) require that licensees must obtain PI insurance cover that is adequate, considering the nature of the licensee's business and its potential liability for compensation claims (reg 7.6.02AAA); or (b) be approved by ASIC as alternative arrangements.

The Corporations Regulations also provide exemptions from the requirements for some licensees that are regulated by the Australian Prudential Regulation Authority (APRA) or are related to an entity regulated by APRA (reg 7.06.02AAA(3)). Such entities are large institutions referred to in the Consultation Paper who often under self-report potential breaches based on, for example, the application of the significance test. There is an expectation that breach reporting from large institutions would increase under the Taskforce's proposed changes.

However, the proposed changes may present implications for the availability and cost of professional indemnity insurance for other parts of the market – namely small and medium licensees, regardless of whether their self-reporting practices change.

It is unclear how PI insurers will respond to changes in the breach reporting requirements. For example, whether reporting changes would result in single claims or a combination of similar claims breaching the aggregate cover for which the licensee is insured for the year and hence would not be covered; or whether insurers would review exclusions based on breach reporting requirements.

Recommendation:

The PI implications of changes to the ASIC breach reporting requirements, particularly for small businesses, need to be carefully considered.

FPA response to Taskforce's preliminary positions

Position 1: The 'significance test' in section 912D of the *Corporations Act 2001* (Cth) should be retained but clarified to ensure that the significance of breaches is determined objectively.

Additional guidance on the significance test is sensible and would be useful. Assuming the guidance is well-formulated it would improve the integrity of the breach reporting system.

However, the significance test should be consumer focused, rather than focused on the impact of the potential breach on the licensee, and able to be applied consistently across the industry regardless of licensee scale, nature, structure, and complexity of the business. Reporting breaches based on consumer focused significance would remove any potential bias in relation to the licensee's size or nature of business, and importantly could change the focus from tick-a-box compliance to improving the quality of advice and services for consumers.

The significance test should encourage licensees to consider whether the conduct subject of the breach is likely to have been repeated with other clients or poses a potential risk for other clients, particularly in large scale organisations. For example, a technical team creates a tax strategy and makes it available to its adviser network. One client receives a tax penalty on the back of the tax strategy. The licensee fails to realise the tax strategy is flawed and identify a systemic breach putting clients across its network at risk.

The guidance should include a definition of 'systemic problem' and clarify when the number and frequency of breaches tips into 'significant'. This may assist in rectifying under reporting.

The consultation paper questions whether it would provide more certainty if all potential breaches were to be reported to ASIC, rather than trying to qualify the significance test. Reporting of all potential breaches, even under a cooperative approach, would result in a significant strain on licensees and ASIC resources, reinforce a compliance driven culture, and create a mini breach reporting industry. Of most concern is the potential for significant breaches to become hidden amongst a massive deluge of insignificant breaches, to the detriment of consumers.

Licensees must be allowed to complete a reasonable level of investigation into the potential breach. This would limit the potential for ASIC to waste resources investigating matters of little benefit to the protection of consumers. If the focus of the test to report moves from determining significance in the eyes of the licensee to a reasonable person test of whether the breach or potential breach has or may have an material impact on the consumer then breaches should be reported to ASIC in a timely manner to investigate.

Recommendation:

The significance test should be retained with consumer focused measures, and additional guidance to ensure breaches can be accurately and objectively assessed in a consistent manner across the industry.

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

The FPA supports measures that improve the transparency of the system and enhance consumer protections by addressing wrongdoing at an organisational and an individual level.

However, it would create a disproportionate impact on an individual's reputation, career, and livelihood if advisers were required to be reported to ASIC by licensees for minor breaches that were not intentional, blatant, fraudulent or reckless. The impact would be equally unjust if an individual was reported to ASIC prior to an investigation being conducted by the licensee to determine if an actual breach has occurred, and the reasons for and significance of the breach identified.

While timely reporting is necessary, there should be a level understanding of the individual's actions that lead to the breach and certainty that the breach was at the hands of the individual and not just a symptom of a broader issue within the licensee, prior to the licensee reporting the individual to ASIC. The tax strategy issue above is a clear example of a systemic issue that came to light via the implementation of the strategy by an individual adviser.

The relevance of some personal information may also require further consideration in relation to the proposal to report breaches made by employees and authorised representatives. For example, is the solvency or bankruptcy status of an employee relevant? What is considered 'good fame' of an employee (criminal traffic offences, drug offences, domestic violence?); and should these be a factor in reporting individual to ASIC in relation to Corporations Act breach reporting requirements?

Consideration should be given to the application of the Australian Privacy Principles in relation to the proposal to report information on employees and authorised representatives to ASIC.

Employees and authorised representatives should be appropriately notified if this change is implemented.

Based on the Consultation Paper, it is unclear as to how the information about an individual representative or employee will be treated and 'held' by ASIC, particularly if the Regulator takes no action against the adviser. For example, will information about the reported breach be held against that individual and/or made publicly available on the ASIC Financial Adviser Register, even if a breach was found to be accidental or did not meet the significance test? How long would ASIC hold such information?

Recommendations:

The FPA supports the inclusion of an obligation for licensees to report to expressly include significant breaches or other significant misconduct by an employee or representative.

This measure should apply to significant breaches of misconduct only and be required after a timely investigation has provided certainty of the individual's misconduct.

Consideration should be given to the application of the Australian Privacy Principles when reporting about an individual representative.

Further consultation should be considered as to how ASIC will treat information reported against an individual representative.

Position 3: Breach to be reported within 10 business days from the time the obligation to report arises. To commence from when the AFSL becomes aware or has a reason to suspect a breach has occurred, may have occurred or may occur, not that the licensee has determined that breach *has* occurred and *is* significant.

Position 6 states that the 10 day timeframe should commence as soon as a licensee has reason to believe a breach 'may have occurred', with the paper noting that many licensees currently exceed the reporting timeframe as their investigation (to establish materiality/significance) takes some time.

Should this proposal be introduced, matters are likely to be reported without a licensee having all the facts to assess against the current significance test, raising the following concerns:

- If a suspected breach is reported, and the licensee's subsequent investigation reveals that the matter is not significant or not a breach, and therefore the information would not have been reportable had all the facts been at hand within the ten day timeframe, how will ASIC treat this information and the licensee in future?

- Will the licensee face the same administrative burden to close out a minor or insignificant breach that has been reported, as it would for a significant or 'actual' breach?

- Would licensee's reports to ASIC that fall into this category remain 'held' and hence become reportable in accordance with Position 12 recommendations for the Regulator to report breaches against licensees?

- If the information relates to an individual employee or representative, would the information be 'held' against the person's record on the relevant ASIC register, such as the Financial Adviser Register (FAR)?

For large licensees there can be significant effort involved in breach reporting. It can take often time (longer than 10 days) to determine if there is an issue and if it is significant. Similarly, it may take time for small licensees to engage an external contractor to investigate the suspected breach.

Introducing a requirement to report every instance a licensee believes may be an issue, will increase the reporting requirements for licensees and transfer effort and resources away from the investigation and resolution of the breach. While it may increase ASIC's ability to identify widespread potential breaches, it will also increase the workload of both the licensee and the Regulator, draining resources away from more significant issues. It will also increase costs on multiple levels for licensees – increased costs of additional reporting requirements; and in the levy incurred under the ASIC Industry Funding Model.

The proposed timeframe of reporting all breaches or suspected breaches regardless of whether significance has been determined within 10 business days from when the AFSL becomes aware or has a reason to suspect a breach has occurred, would not encourage early reporting as it does not allow the licensee to exercise its own due process to investigate the matter sufficiently to determine if a breach exists and has the potential to increase the reporting of suspicions where no breach is then found or the significance test met.

There must be a balance between timeframes for breach reporting, the necessity to allow due investigative processes to take place, transparency and the need to limit unnecessary strain on finite

licensee and Regulator resources. A staged approach with a reporting timetable in place of a rigid 10 day reporting requirement may achieve greater balance and better outcomes for consumers.

If the requirement to report first, investigate second, as per Position 6 is introduced, we submit that ASIC requires appropriate processes to treat the licensee fairly, including a process to revoke or dismiss an early breach report, should the matter not eventuate as a breach.

If the focus of the test to report moves from determining significance in the eyes of the licensee to a reasonable person test of whether the breach or potential breach has or may have an material impact on the consumer, then breaches should be reported to ASIC in a timely manner to investigate.

The Consultation Paper states that a "licensee could be deemed to be aware of the facts and circumstances that established the breach, suspected breach or potential breach where the licensee has received that information from any of the following:

- a government agency;
- its auditor;
- an industry Ombudsman, or other body to which the licensee must belong under its external dispute resolution scheme obligations; and/or
- 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.

It should also state that consumers are able to make licensees aware of a potential breach.

Recommendations:

Consider a staged approach reporting timetable in place of a rigid 10 day reporting requirement, to allow due investigative processes to take place, improve transparency of the breach reporting system, and limit unnecessary strain on finite licensee and Regulator resources.

If Position 6 is introduced, ASIC should be required to adhere to appropriate processes to treat licensees fairly, including a process to revoke or dismiss an early breach report should the matter not eventuate as a breach.

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

The proposal to increase the monetary and custodial penalties to the maximum criminal penalty for a failure to report breaches in a timely fashion is tabled to deter deliberate non-compliance with the reporting obligation. This reinforces that the focus of the Consultation Paper and proposals are based on the behaviour of certain large licensees. There is no evidence in the paper that there is a systemic failure of the industry as a whole.

The proposed penalties and fines do not appear to make a distinction between large and small licensees to provide a sufficient incentive to report, or the consequence of not reporting. For example if the fine for not reporting a breach was $1million this would definitely encourage small licensees to report early as the impact to the licensee is substantial. However, a $1million fine for not reporting for a large licensee may not be a significant incentive to report a potential breach in a timely manner. As such, penalties and fines should be scaled based on the licensee's size or balance sheet.

The size of the penalty or fine should also be proportionate to the significance of the breach which has not been reported or the level of action taken by the licensee to remedy the breach.

Sanctions must be proportional to the conduct.

Recommendation:

Increased penalties should apply to a blatant failure to report significant breaches, in particular misconduct and fraud.

Penalties and fines should be scaled based on the licensee's size or balance sheet, and proportionate to the significance of the breach which has not been reported or the level of action taken by the licensee to remedy the breach.

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

We note that the details of a civil penalty in addition to the criminal offence for failure to report, is to be the subject of a separate review by the Taskforce.

Civil sanctions and penalties would be an effective method to encourage appropriate self-reporting, however there must be sufficient time allowed to complete internal due process, and the size of the penalties must be proportionate to licensee size and breach significance.

If civil penalties or fines are to be introduced, apart from noting the size of the penalty being relative to the size of the licensee, the size of the penalty or fine should also be proportionate to the significance of the breach which has not been reported or the level of action taken by the licensee to remedy the breach.

The FPA supports this measure and will participate in the planned consultation.

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

We note that the details of an infringement notice regime for simple or minor contraventions that do not involve a deliberate failure to report, is to be the subject of a separate review by the Taskforce.

The FPA supports this measure and will participate in the planned consultation.

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

The issues of the current reporting system highlighted in the Consultation Paper are exacerbated by the response of the Regulator as experienced by licensees. ASIC currently take significant time to notify the licensee as to how the Regulator will treat the information reported – whether ASIC will look into the potential breach or let it go.

This leaves licensees in the dark, worrying about the Regulator's potential action, making licensees reluctant to report borderline potential breaches in the future. This experience may impact on the

industry's openness to adopting a cooperative approach to breach reporting, and also reinforces the tick-a-box approach to compliance.

However, a cooperative approach to encourage early reporting may offer benefits to licensees, ASIC and consumers. We note the Taskforce's proposal includes:

- 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, and giving the licensee an opportunity to complete its investigations.

- No ASIC action against the licensee if the licensee cooperates with ASIC and addresses the matter to ASIC's satisfaction by:

    - the breach report sets out a program to address the matter including completion of any further investigations and the manner in which the licensee will rectify or remediate the matter;

    - the program includes regular time frames for the provision of additional information to ASIC;

    - the program has clear time frames for implementation and completion;

    - the program will resolve the matter to the satisfaction of ASIC; and

    - the program is implemented to the satisfaction of ASIC.

The standard requirement is to report significant breaches within 10 business days, which requires licensees to determine if a potential breach meets the significance test. It is assumed therefore, that for the ASIC No Action option to apply, early reporting would be required to be done within a significantly reduced timeframe. However, the conditions that are required to be met when reporting early are potentially onerous and time consuming, greatly reducing the ability of licensees to meet the early reporting requirements.

It may be more useful if:

- ASIC develop guidance including standard program timelines and requirements for investigation and information provision, in consultation with industry, for licensees to rely on when reporting early, and

- If a licensee cannot meet the ASIC guidance on early reporting conditions, no penalty should be imposed if reasonable warning is provided to ASIC with a tailored program including the frequency of information updates and an investigation program.

The early reporting conditions for ASIC No Action should recognise the differing levels of investigation related to minor and non-systemic potential breaches, versus more serious or systemic issues which involve more resources and usually require longer timeframes for investigation.

Consideration could also be given to the following alternatives, which could limit the potential for ASIC to waste resources investigating matters of little benefit to the protection of consumers:

- the timeframe to report any breaches, or potential breaches which are not considered significant, should be extended to a longer timeframe (say 45 or 60 days), or

- the breach register of all licensees to be provided to ASIC on a regular basis (say quarterly or half yearly) to allow the licensees to complete a reasonable level of investigation into the potential breach so it can report to ASIC the action or proposed action to remedy the breach.

While incentives such as discount in the penalty for an underlying breach and taking the reporting into consideration when considering liability and civil penalties, it also risks introducing a level of discretion that could be unfairly applied.

Consideration should be given to the objective behind introducing an early reporting incentive program into the breach reporting system. While a cooperative approach is desired and positive, early reporting incentives may do little to change the behaviour of licensees who are not already predisposed to reporting to ASIC and also drain limited licensee and ASIC resources with little benefit to consumers.

Recommendation:

While a cooperative approach is supported, requiring and incentivising early reporting may drain resources and not be in the best interest of consumers.

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

As stated in ASIC's Report 515:

> *"In the past, the institutions have relied on traditional monitoring and supervision tools, such as customer complaints data or adviser audit outcomes, to identify which advisers pose a higher risk of non-compliant conduct (high-risk advisers). More recently… the institutions have been using new technologies and data analytics to develop key risk indicators (KRIs) to assist in identifying high-risk advisers and affected customers. This will contribute to more effective monitoring and supervision.*
>
> *When developing these KRIs, the institutions faced challenges because of the limitations on data collection and retention. Some of the reasons observed for these limitations included that:*
>
> *(a) older data was less reliable, unavailable or non-existent;*
>
> *(b) paper-based record keeping made information more difficult to access;*
>
> *(c) incompatible legacy systems, resulting from technology upgrades and business mergers, made data extraction difficult; and*
>
> *(d) different data-recording methods were used within the institutions and across their different licensees*
>
> *Nevertheless, we think that the development and use of KRIs, and enhanced records and data management, appropriate to the licensee's business, can assist in identifying high-risk advisers and affected customers.*[4]

[4] para 25-28 pg 8

> *From our engagement with the institutions, we observed that significant resources have been allocated to the development and improvement of data systems and data analytic tools. These changes range from the centralisation of their licensees' data records, through to their transition from paper-based to digital record keeping.*[5]

However, it is important to bear in mind that ASIC's Report 515 was based on findings at 5 large licensees who have the scale and need to implement such new technologies and data analytics across the extreme breadth of their business operations due to the arm's length relationship they hold with most of their representatives.

Small and to some extent medium licensees, have a closer relationship and therefore oversight of their representatives. They are also more likely to use independent compliance consultants.

While technology can offer many benefits, requiring licensees to introduce and use new technologies and data analytics may be cost prohibitive for small and medium licensees. Consideration should be given as to how ASIC's systems could be enhanced to provide an appropriate data reporting gateway for licensees.

Currently a licensee is required to maintain a breach register covering all representatives within the licensee and the onus is on the licensee to notify ASIC in writing when the licensee determines the breach is (or likely to be) a significant breach. Lodging breach reporting electronically would assist licensees provided it replaces the current breach register system which is managed by the licensee. The current breach register process should be replaced with an online facility managed by ASIC so a consistent reporting process can be implemented across the industry.

Prescribing the content to be included in breach reports is sensible, will improve transparency, and could assist ASIC to utilise data analytics. However, prescribed breach report content requirements must be used consistently by all licensees for it to be effective and fair.

Recommendation:

The required content of breach reports be prescribed and required to be delivered electronically, via a system managed by ASIC.

Consideration must be given as to how ASIC's systems can help support small and medium licensees to meet electronic reporting requirements.

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

The Consultation Paper indicates that qualified privilege would need to continue to apply to licensees if the breach reporting requirements were changed, to ensure licensees are protected from third party liability when self-reporting to ASIC in good faith.

However, unwaivering qualified privilege raises concerns about licensee power and intimidation toward employees and representatives, particularly in the context where the (advice) corporation has no formal duty to the public interest as embodied in notions of professional duty.

[5] Pg 13

There is a need to consider options to overcome this risk such as (for example):

- anti-intimidation provisions specifically attached to the application of the qualified privilege, or
- a two-tier breach reporting obligation that gives qualified privilege to an individual – that is whistleblower protection for employees and representatives, directors and responsible managers (Individuals who would otherwise have personal liability to the civil penalty regime or worse under Ch 7 or the ASIC Act, who reports a matter to the corporation).

There is also a need to ensure qualified privilege is appropriately applied. For example, ASIC (via REP515) expects licensees to report to their advisers who have been classified as a 'Serious Compliance Concern' (SCC advisers) notwithstanding that they may not fit the definition / guidance around significant breach reporting obligations under s912D. The challenge this poses is that a voluntary notice to ASIC is not covered by privilege and hence is available to third parties leaving the door open for defamation cases.

If ASIC continue to require licensees to report any SCC advisers, consideration should be given to whether the breach reporting obligations should be extended to formally include the reporting of SCC advisers so that qualified privilege can apply. This should include a clear definition of SCC advisers.

Qualified privilege under the current breach reporting process should be extended across the entire spectrum of the breach reporting and investigation process until an individual or licensee is determined guilty of a significant breach. The lack of an appropriate level of privilege runs the risk of an individual's or licensee's reputation being damaged when no breach may have actually taken place (especially if early reporting of potential breaches is introduced, as per the Taskforce proposal) or if the breach is administrative or accidental in nature.

Recommendation:

Qualified privilege for licensees from third party liability when self-reporting to ASIC is necessary, and should extend across the entire spectrum of the breach reporting and investigation process until an individual or licensee is determined guilty of a significant breach.

Representatives and employees should be afforded protection from the risk of intimidation because of the qualified privilege afforded to the licensee.

Clarification is needed regarding the application of qualified privilege when reporting SCC advisers to ASIC.

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

Position 12 suggests that reporting firm-wide breach data could be made public. This could include the licensee name and number of breaches for the reporting period.

Placing licensee level data in the public domain comes with significant risks including:

- consumer misunderstanding or misinterpretation of the data
- media misrepresentation
- breach occurrences taken out of context

The most significant risk is the potential for extreme and potentially unjust reputational damage. While large licensees can use their scale and diversity to shield themselves from such a risk as demonstrated from recent failings in the banking sector, medium and small licensees in particular are reliant on a strong reputation for the survival of their business.

Although the format in which ASIC reports data would be innocuous, the potential for media use to harm the reputation of licensees and cause consumer concern is significant. The many stories tarnishing the whole financial advice profession off the back of the conduct of certain large licensees as reported by Adele Ferguson and 4 Corners, are a simple example of the reputational impact at stake for any licensee who would be named if ASIC was required to report breach data.

The threat to a licensee of data reporting will also reinforce a tick-a-box driven approach to compliance to reduce breach reporting, rather than on improving the quality of financial advice and services for consumers.

Whether a breach or potential breach is reported is heavily dependent on a licensee's application of the breach significance test and approach to compliance. Some licensees may err on the side of caution and report even borderline breaches, while others may take a different approach. This will unfairly impact on the licensee doing the right thing as it will result in increased data held and reported by ASIC under this proposal.

It is important to consider this proposed Position in the context of Position 6. Position 6 would require licensees to report potential breaches first, and investigate whether an actual breach has occurred second. If all matters reported to ASIC are 'held' even where a subsequent investigation reveals no actual breach occurred, the data that is reported by ASIC will be inaccurate and misleading, to the potential detriment of the licensee.

Reporting a breach is not necessarily a reflection on the state of operations at the licensee or the quality of the advice and services provided to consumers. It seems potentially unfair that a working compliance regime could result in 'bad' publicity.

This data is likely to be misused or misunderstood unless there is clear differentiation between the severity of the matters being published. Increasing transparency can be good, however there is a high risk that statistics are likely to be misused.

The proposed thresholds for publicising data based on the total number of breaches reported, with a suggestion of those with over 500 breaches be publicly reported by ASIC, also indicates that the proposed Positions are aimed primarily at very large licensees. However, the impact of the misuse and misinterpretation of reported data would be felt across the industry.

The nature, complexity, culture, scale, and service offerings vary significantly from licensee to licensee, as do any potential breaches and the significance of each breach. That is, a breach by one licensee may have different impacts, severity and significance to the same breach by another licensee. However, ASIC breach data may unfairly be used as a tool for comparing licensee performance.

Releasing breach reporting data into the public domain inappropriately reflects ASIC's use of naming and shaming as a penalty against licensees and representatives where a case of misconduct has been investigated and proven.

It is also unclear how such data will be reported in relation to records accessed via ASIC's registers such as the licensee register and the Financial Adviser Register.

However, it would be appropriate for ASIC to report industry level findings annually to give the public confidence that the profession is being adequately monitored and policed. This data should be generic only and give reference to the size of the advice market overall. For example, ASIC convicted 3 advisers or licensees of significant breaches across an advice market of 16,000 authorised representative. This would put the level of breaching in perspective. Unless a 'naming and shaming' sanction has been imposed, the data should not name licensees as the actions of a minority group of advisers or single adviser could have detrimental damage on those compliant and competent advisers of that licensee. Data should trends or areas of concerns to enable education and improvement across the entire advice market. If reporting of advisers or licensees to the market is being considered, it should be confined to those responsible for the breach – that is, if it is an individual adviser issue the adviser only (not licensee) should be named.

Recommendation:

The FPA opposes the publication of firm wide breach data by ASIC.