SUBMISSION

Submission to Treasury — Strengthening breach reporting

28 February 2020

The Association of Superannuation Funds of Australia Limited
Level 11, 77 Castlereagh Street
Sydney NSW 2000

PO Box 1485
Sydney NSW 2001

T +61 2 9264 9300
1800 812 798 (outside Sydney)
F 1300 926 484
W www.superannuation.asn.au

ABN 29 002 786 290 CAN 002 786 290

File: 2020/08

Senior Adviser
Consumer and Corporations Policy Division
Treasury
Langton Cres
Parkes ACT 2600

Via email: FSRCconsultations@treasury.gov.au

28 February 2020

Dear Sir/Madam

Royal Commission Recommendations 1.6, 2.7, 2.8, 2.9 & 7.2 – Strengthening Breach Reporting

The Association of Superannuation Funds of Australia (ASFA) is pleased to provide this submission in response to the exposure draft legislation released on 31 January to implement recommendations 1.6, 2.7, 2.8, 2.9 and 7.2 of the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry.

About ASFA

ASFA is a non-profit, non-political national organisation whose mission is to continuously improve the superannuation system, so all Australians can enjoy a comfortable and dignified retirement. We focus on the issues that affect the entire Australian superannuation system and its $2.9 trillion in retirement savings. Our membership is across all parts of the industry, including corporate, public sector, industry and retail superannuation funds, and associated service providers, representing almost 90 per cent of the 16 million Australians with superannuation.

If you have any queries or comments in relation to the content of our submission, please contact me on (03) 9225 4021 or by email fgalbraith@superannuation.asn.au. We acknowledge that the deadlines for this consultation are tight but we would welcome the opportunity to discuss our submission with you if time permits.

Yours sincerely

Fiona Galbraith
Director, Policy

General comments

ASFA generally is supportive, in principle, of the objectives of the proposal and the draft bill to implement recommendations 2.8 and 7.2 of the Royal Commissions.

We recognise the importance of a strong regime with respect to the reporting of breaches and the completion of investigations and remediation, including the self-reporting by financial services licensees of contraventions.

Members have, however, raised some concerns – in particular that:

- it is imperative that the scope and 'trigger' for the self-reporting obligations are clarified
- the imposition of differing reporting obligations as between APRA and ASIC will create significant practical difficulties and a material, additional compliance burden for dual-regulated entities.

The level of guidance provided by the regulators will be critical to the successful implementation of the reforms.

Specific comments in relation to the exposure draft legislation

Reporting of investigations

No definition of 'investigation'

The proposed breach reporting obligations introduce the concept of a new reporting event which necessitates the reporting of 'investigations' into potential breaches of core obligations.

There is, however, no definition of 'investigation'.

By way of example, does the making of a complaint at the beginning of a complaints process, or initial 'fact finding', constitute an 'investigation'?

In the absence of a definition it would appear that the open definition of 'investigation' would require a licensee to report **all** investigations to ASIC irrespective of materiality, size, scope or significance. This would introduce a significant overhead with respect to reporting the initiating event, together with all outcomes, regardless of whether they are determined to be significant, and in a number of instances is likely to lead to duplicate reporting of both investigation and breach.

Without a definition, the requirements to report matters with respect to 'investigations' to ASIC potentially will apply to a broad range of activities conducted by governance, risk, legal and compliance functions and advisers, including minor and insignificant activities.

Recommendation
Definition of investigation It is essential that clarity as to the scope and definition of the concept of an 'investigation' is provided, to prevent unnecessary reporting of volumes of insignificant / immaterial matters.

Investigations only need be reported if likely breach significant

According to the Explanatory Memorandum:

> *"breaches and likely breaches of core obligations, and investigations of such, only need to be reported if the breach or likely breach is significant".*

At the commencement of an investigation, however, it is impossible to determine whether the incident is a significant breach.

Further, it is unclear whether all investigations are expected to be reported within 30 days, including those that have been investigated and where it was concluded that no breach has occurred. This will need to be clarified but we submit that, where no breach has occurred, an investigation should not need to be reported.

If a licensee will be required to report the number of investigations it undertakes it will be important that the public reporting also include information with respect to how many investigations identified breaches and how many found there to be no breach.

Recommendation

Reporting of investigations

The requirement to report investigations should apply only in circumstances where:

- a breach is being investigated by the licensee; AND
- the investigation has not concluded within the prescribed time limit of 30 days.

Where the licensee determines, during the period of investigation, that no significant breach has occurred, there would be no obligation to report to ASIC.

When does a licensee know, or have reasonable grounds to believe, a reportable situation has arisen

Example 2.2 of the Explanatory Memorandum provides practical guidance as to when a licensee is taken to have reasonable grounds to believe a reportable situation has arisen.

The example implies that a licensee or person 'knowing, or reasonably knowing, that something has taken place' does not appear to have occurred until a 'senior staff member' has been made aware by being provided with a report on the matter.

We submit that the legislation (or alternatively a subsequent regulatory guide) should clarify explicitly that a licensee or person 'knowing, or reasonably knowing, that something has taken place' has not occurred until a 'senior staff member' has been made aware of the matter.

Ideally 'senior staff member' would be defined in a similar manner to the individuals accountable under the BEAR and proposed FAR regimes.

Recommendation

'Knowing, or reasonably knowing' that something has taken place

The legislation, or a regulatory guide, should clarify that a licensee or person 'knowing, or reasonably knowing, that something has taken place' has not occurred until a 'senior staff member' has been made aware of the matter.

Reporting of breaches

Definition of 'significant'

Under subsection 912D(1) a breach, or likely breach, of a core obligation that is significant must be reported.

Under subsection 912D(5)(c) such a breach is taken to be 'significant' if it relates to a provision that attracts a criminal conviction (of the type specified in the legislation), civil penalty or results in loss or damage to clients. This potentially captures **any** loss or damage.

No guidance as to 'loss or damage to clients' and absence of materiality threshold

In the absence of a materiality threshold for the reporting of breaches, or guidance as to what is considered to constitute 'loss or damage to clients' for the purpose of breach reporting, all instances of loss or damage, irrespective of size, will need to be reported at first instance.

Our primary concern is that applying the reporting obligation regime to all breaches which contravene the civil penalties regime, or that cause loss or damage to a client, will result in an inordinate number of small, relatively immaterial or minor technical breaches being required to be reported to ASIC.

With respect to 'loss', we note that the Taskforce recommendation was that the criteria should be 'potential **material** loss to client' – the proposed legislative drafting 'loss to client' is inconsistent with this and would deem all client losses to be significant.

The concept of damage is not defined. While the Taskforce recommendations provided some guidance as to what might constitute damage, without clarity as to the definition of 'damage' this introduces a subjective element to this criterion.

The absence of suitable definitions / guidance or a materiality threshold will lead to the over-reporting of investigations and breaches, a significant increase in the time and resources involved in the reporting of investigations and breaches, a consequential rise in overhead costs and significant inefficiencies for both industry participants and ASIC.

Examples of matters which happen from time to time and are quickly and easily rectified include:

- a member under advice may exceed a contributions cap
- a Fee Disclosure Statement may be provided a day late
- a Financial Services Guide may not be given at an initial, exploratory meeting.

By way of contrast, currently unit pricing errors below $20 do not have not have to be reported. This is an example of the existence of a sensible materiality threshold.

Recommendation

Reporting of breaches

The obligation to report breaches should be limited to circumstances where an investigation has found, or there are reasonable grounds to believe, that:

- a core obligation may have been breached; and
- the breach is significant.

There should be a concept of materiality applied to determine whether 'loss or damage to clients' is significant in the circumstances.

Timeframe for reporting - matters within 30 calendar days/outcomes of investigations 10 calendar days

Members are concerned that 'calendar days' includes holiday periods and weekends and that as the requirement pertains to the running of a business, 'business days' should be utilised instead.

Recommendation

Reporting timeframes

'Business days' should be utilised instead of 'calendar days'

Commencement of new breach reporting provisions

The new breach reporting provisions apply to breaches, or likely breaches, occurring from 1 April 2021.

'Occurring' may need to be defined to clarify whether it refers to a reasonable suspicion or reasonable knowledge being formed or an investigation being commenced.

By way of example; if an incident occurred prior to 1 April 2021, but is detected on or after 1 April 2021, will these new breach reporting requirements apply?

Reporting both investigations and breaches

The requirement to lodge reports at multiple points about investigations and breaches creates unnecessary and avoidable complexity and duplication, with an increased risk of a particular report not being lodged due to an unintentional oversight.

There is no clear policy rationale for lodging multiple reports with respect to the same matter.

Recommendation

Reporting of investigations and breaches

As stated above, we recommend that:

- the requirement to report investigations should apply only in circumstances where
    - a breach is being investigated by the licensee; AND
    - the investigation has not concluded within the prescribed time limit of 30 days
- where the licensee determines, during the period of investigation, that no significant breach has occurred, there would be no obligation to report to ASIC
- where the investigation finds, or has reasonable grounds to believe, that:
    - a core obligation may have been breached
    - the breach is, or would be, significant

  there would be an obligation to report the breach.

Reportable situations and additional reportable situations

Lack of clarity / definitions

A report is required to be provided when a person 'reasonably knows' there are reasonable grounds that a reportable situation, or an additional reportable situation, has arisen.

The definition of 'reasonably knows' includes where a person is aware of 'substantial risk' and it is 'unjustifiable to take the risk'.

These terms need to be defined.

Further, draft sub-paragraph 912DAA(1)(b) refers to a person being aware of a substantial risk that the circumstances exist or will exist. We query the legislative intent of this section above and beyond what is captured under sub-paragraph 912DAA(1)(a).

In addition we do not believe that the statement that 'the taking a risk is unjustifiable is one of fact' is especially instructive or helpful for industry. This needs to be expressed / explained better and to be supported by the provision of guidance through a regulatory guide.

'Additional reportable situation' can include 'gross negligence' or fraud.

Determining gross negligence would necessitate a subjective judgement by the licensee. Members have raised concerns that the term 'gross negligence' is not defined and not used widely in Australia, so there would be limited guidance provided under case law.

Interaction with whistle blower regimes

The types of reportable situations captured by the proposed new breach reporting requirements potentially may also trigger obligations under different whistleblower regimes.

Recommendation

'Reportable situation'

There should be guidance and information with respect to the interplay of the obligations with respect to 'reportable situations' and those under the different whistle blowing regulatory regimes.

Penalty regime

Failure to lodge a report - penalty

An entity must comply with its licensing obligations – an offence can attract a penalty.

Failure to lodge a report in accordance with the self-reporting obligations is an offence which attracts a maximum penalty of 2 years imprisonment.

This penalty is quite significant and may have unintended consequences.

To whom does penalty apply?

Members have been seeking confirmation as to whom this obligation applies – the directors of the licensee or an individual with responsibility for compliance with regulatory obligations as part of their role?

Effect of potential unduly punitive penalty regime on ability to attract talent

The nature and scope of the penalty regime may have a significant impact on the ability of APRA-regulated entities to attract talent, including from entities outside the regulatory remit of APRA and ASIC, while for global talent the possible imposition of penalties may act as a deterrent to taking up a position within the Australian financial services sector. The potential for the imposition of penalties may serve to increase remuneration expectations and, by extension, costs to members.

Unintended consequences of unduly punitive penalty regime

There is a considerable risk that there may be unintended consequences of these measures.

In particular there is a risk that the breach reporting process may be undermined with employees and advisers reluctant to report a potential or suspected breach. At best parties may 'pick up the phone' in lieu

of creating any documentation lest it be considered to be an 'investigation' – at worst they may say nothing at all.

Recommendation

Penalty regime

The penalty regime should be less punitive.

ASIC prescribed form of breach reporting

We note that ASIC is looking at introducing a prescribed form of breach report, in which case reports must be lodged in the form prescribed or approved by ASIC.

ASIC has not yet indicated what information will be required to be disclosed.

It would be extremely useful for trustee to obtain further information about this – ideally a 'mocked up' version of the form – in advance as many licensees may need to change their breach reporting forms (often configured as part of a third party risk and compliance system) to meet these requirements.

Recommendation

ASIC prescribed form of breach reporting

ASIC should provide further information about its prescribed form of breach reporting – ideally a 'mocked up' version of the form – as soon as possible.

Publication of information about significant breach reports lodged

ASIC will be required to publish information about reports lodged about significant breaches, and likely breaches, of core obligations during the financial year.

ASIC has discretion with respect to the content and form of this publication, but potentially it could include the name of the licensee and the volume of reported breaches.

While we appreciate the need for transparency, the publication of this type of information, without the inclusion of further information such as remedial steps or treatment actions, would not present a full and complete picture.

ASFA is supportive of not providing names as part of public reporting, as we believe this could drive inappropriate behaviour, such as not reporting matters as 'knee jerk reaction' to protect reputations.

Furthermore – if licensees will be required to report the number of investigations undertaken – it will be important that the public reporting include information with respect to how many investigations identified breaches and how many found there to be no breach.

If breach reports are required to be lodged for a likely breach as well as an actual breach with respect to the same matter this will distort the data and provide an inaccurate picture of the true number of significant breaches.

Recommendation

Publication

The publication of information with respect to significant breach reports lodged should be generalised information.

If licensees are required to report investigations undertaken, public reporting must include information with respect to how many investigations identified breaches and how many found there to be no breach.

If breach reports are required to be lodged for a likely breach as well as an actual breach, with respect to the same matter, the data must be adjusted to provide an accurate picture of the true number of significant breaches.