File Name: 2015/01

16 January 2015

Mr Pat Brennan
General Manager, Policy Development
Policy, Statistics & International Division
Australian Prudential Regulation Authority
GPO Box 9836
SYDNEY NSW 2001

Email: superannuation.policy@apra.gov.au

Dear Mr Brennan

Consultation on Draft SPG 223 – Fraud Risk Management

The Association of Superannuation Funds of Australia (ASFA) is pleased to provide this submission in relation to draft Prudential Practice Guide SPG 223 – *Fraud Risk Management* released by the Australian Prudential Regulation Authority (APRA) on 27 October 2014.

We note that, as with the other prudential practice guides that APRA has released, the intent of SPG 223 is to include practical guidance to Registrable Superannuation Entity (RSE) licensees from the Regulator on matters regarding the management of fraud risk in support of the prudential requirements set out in Prudential Standard SPS 220 – *Risk Management* (SPS 220). In that context, it is understood that SPG 223 is intended to provide guidance on APRA's view of sound practice in this area and does not create enforceable obligations or requirements.

ASFA has consulted with its members and reviewed draft SPG 223. Our comments are set out in this submission.

About ASFA

ASFA is a non-profit, non-politically aligned national organisation. We are the peak policy and research body for the superannuation sector. Our mandate is to develop and advocate policy in the best long-term interest of fund members. Our membership, which includes corporate, public sector, industry and retail superannuation funds, plus self-managed superannuation funds and small APRA funds through its service provider membership, represent over 90% of the 12 million Australians with superannuation.

General comments

As an overall comment, ASFA is broadly comfortable with the contents of draft SPG 223. In our view, the guide will assist an RSE licensee in complying with the requirements set out in SPS 220 to have systems in place for identifying, assessing and managing material risks and to develop prudent practices in relation to the management of fraud risk.

We note that draft SPG 223 uses the terminology "APRA expects" in a number of places. ASFA's view is that, given the fact that prudential practice guides do not contain enforceable requirements, where an RSE licensee's process does not accord with APRA's expectations, it should be sufficient for an RSE licensee to evidence:

- an awareness and consideration of APRA expectations; and
- an alternative justifiable position.

Specific comments

The remainder of this submission outlines ASFA's feedback in relation to specific sections of draft SPG 223 for your consideration.

Paragraph 11 – Supplemental guidance

Paragraph 11 states that "[a] prudent RSE licensee would supplement the guidance outlined in this PPG with external sources of information relating to the development and implementation of a fraud risk management framework".

ASFA supports this statement on the basis that there is significant guidance already available to RSE licensees in this area, including Australian Standard AS 8001-2008 – *"Fraud and Corruption Control"* as well as ASFA Best Practice Paper No.20 – "*Managing the risk of fraud and corruption in superannuation funds*" (ASFA BPP No.20).

In particular, ASFA BPP No.20 sets out in detail the various aspects that we believe should comprise an effective fraud risk management framework as well as 24 'best practice' recommendations aimed at assisting RSE licensees in managing the risk of fraud and corruption. Given the general nature of the guidance contained within draft SPG 223, it may be worth emphasising the more detailed nature of the guidance that exists elsewhere.

Paragraphs 50 and 51 – Outsourcing risks

Paragraphs 50 and 51 outline the need for an RSE licensee to address its exposure to fraud risk as a result of engaging outsourced service providers to undertake material activities with respect to the RSE.

ASFA suggests that this section of the paper could be expanded to provide further guidance to RSE licensees in the following areas:

i. Selection of outsourced providers

RSE licensees should consider the following matters prior to the selection of an outsourced service provider:

- Organisational culture and executive support, including matters such as average service period of staff, degree of staff turnover and adequacy of training programs offered
- Requirement for full disclosure of fraud management and history
- Control effectiveness – ensuring that providers review the effectiveness of fraud controls on a regular basis to determine whether they adequately mitigate fraud risk, including the use of external reviewers

- Sophistication of the external provider's IT systems – eg. the extent of manual workarounds
- Experience/track record in servicing similar fund(s), including demonstrated ability and capacity to process the level of complexities and/or volume of transactions and the additional volumes should they be selected
- Right of access – i.e. the ability for the RSE licensee, or its appointed delegates or agents, to make site visits to the outsourced provider
- Internal audit and assurance – i.e. determination of the effectiveness of the outsourced provider's internal audit function and a review of its reports
- External audit and assurance – review of the external party's external audit reports
- Financial stability – evaluation of the external party's asset backing and insurance arrangements to determine if they are sufficient to cover payment for damages that may arise from breaches for which the external party bears legal responsibility
- Extent of outsourcing by the outsourced provider and the adequacy of monitoring by the outsourced provider
- Impact of differing legal jurisdictions, especially where the function is being performed in a foreign jurisdiction.

ii. Engagement contracts

RSE licensees should ensure all outsourced arrangements are documented in contracts which set out the requirement for the outsourced provider to provide reports (regular, exception and on-demand) to the RSE licensee on the effectiveness of their risk management controls and any incidents of suspected or actual fraud involving any client.

The RSE licensee should review what information is required, how often it is required and when, in order to confirm that the arrangements will ensure these requirements are achievable. There should be provision to make reasonable requests for ad hoc reports and to agree on changes and additions to reporting from time to time.

iii. Monitoring and supervision of third parties

Ongoing monitoring and supervision of outsourced providers in relation to fraud should be established to ensure that the fraud risk management controls remain adequate and are operating effectively. This should include:

- a risk assessment conducted as part of the selection process and assessment of their fraud control plan
- as stated in *(ii)* above, it is essential that the RSE licensee has access to all necessary reports and documentation from outsourced providers in order for the RSE licensee to meet its statutory and fiduciary obligations to effectively monitor and supervise its outsourced providers
- ensuring that the quality of all regular and ad-hoc reports (including reporting on Service Level Agreements, onsite visits and breach reporting) provided by the outsourced provider are reviewed and any deficiencies in their systems, controls or reporting are addressed.

iv. Loss recovery

An RSE licensee should ensure that, in the event of loss arising from fraud, any claim can be initiated under the outsourcing contract, professional indemnity or other insurance policy.

Where a loss is suffered through the action, or inaction, of an outsourced provider, and not through the actions of an RSE licensee, the loss generally will not be covered under the trustee liability insurance policy. The outsourcing contract should have indemnity provisions dealing with this situation.

Attachment B – Examples of fraud controls

Attachment B provides examples of fraud prevention controls and fraud detection controls, which we believe contain very useful guidance for RSE licensees in these areas. However, ASFA suggests that consideration be given to expanding this section to include examples of appropriate fraud response/management controls as well.

When a suspected fraud is detected, investigation procedures are key to a successful response. Examples of useful controls that could assist an RSE licensee, beyond prevention and detection, include:

- Event management controls (which may be part of the fraud control plan or equivalent) to respond to member, employer and/or media enquiries, internal communication to responsible persons and other staff, and communications with law enforcement and regulators.

- Controls for recording and escalating all suspicions of fraud and corruption including:
    - ensuring all suspicions and instances of fraud and corruption are recorded in a fraud incident report or an incident/breach register; and
    - ensuring all such instances are reported to senior management, the Audit/Risk and Compliance Committee (where applicable) and the Board.

- Controls to respond to, and investigate, fraud or suspicious activity including:
    - considering what skills are available in-house for the investigation (an RSE licensee needs to be aware of the specialised skills required);
    - appointing the person(s) who will be responsible for leading the investigation (investigative officer(s));
    - contact details for external experts who could assist in an investigation;
    - detailed steps and procedures to be followed (which should be outlined in the fraud control plan or a separate document);
    - clear processes around what steps the investigative officer(s) must undertake when a particular event/activity arouses their suspicion, including the process to be followed where the person under suspicion is a trustee director or a member of senior management;

- particularly in cases of internal fraud, steps to be taken to secure and preserve evidence for potential prosecution while not alerting the suspect(s);
- dealing with suspects, including when/if the suspect is informed of the allegation, suspension and termination procedures etc;
- dealing with an informant/whistleblower, including protecting their anonymity and keeping them informed of progress of the investigation;
- ensuring confidentiality of information to avoid defamation of innocent parties;
- process for escalating and reporting internally;
- formal procedures for determining whether an appropriate law enforcement agency should be involved and, if so, the process for involving the agency;
- procedures and timing for notifying insurers of a fraud or potential fraud;
- procedures and timing for advising the relevant regulator(s)
- disciplinary policies and procedures;
- legal advice to determine what action can be taken to recover monies from the individual(s) responsible and/or lodging a claim with the RSE licensee's trustee liability insurer; and
- post-fraud event review of the RSE licensee's fraud risk management framework, including evaluating the effectiveness of the fraud risk controls and making adjustments if required.

* * * * *

I trust that the information contained in this submission is of value. If you have any queries or comments regarding the contents of our submission, please contact ASFA's Senior Policy Adviser, Jon Echevarria, on (02) 8079 0859 or by email jechevarria@superannuation.asn.au.

Yours sincerely

Fiona Galbraith
Director, Policy