AUSTRALIAN PRUDENTIAL REGULATION AUTHORITY

1 Martin Place (Level 12), Sydney, NSW, 2000
GPO Box 9836, Sydney, NSW, 2001

T 02 9210 3000 | W www.apra.gov.au

HELEN ROWELL
Deputy Chairman

31 October 2016

To: All RSE licensees

INFORMATION SECURITY

APRA has observed increased appetite by participants within the superannuation industry to develop and implement new business practices. This includes aspects of administration, communication and account consolidation practices that are generally driven by new technologies, with increased reliance on electronic communication and (in some cases) outsourcing to non-traditional service providers.

Whilst innovative approaches to engagement with members are encouraged, it is essential that RSE licensees appropriately identify, assess and manage the associated risks of new business processes. This includes a prudent assessment of the materiality of arrangements with outsourced service providers, with a particular focus on ensuring the security of member data.

Electronic direct marketing to superannuation account holders

As you may be aware, the Australian Taxation Office (ATO) recently wrote to all RSE licensees (ATO Letter) regarding sending unsolicited bulk email and/or SMS messages to members for the purpose of enrolling them in superannuation account search and retrieval schemes using the ATO's SuperMatch2 portal. The ATO's letter outlined important principles which APRA expects to be applied more generally in relation to member communication and information security. APRA shares the concerns raised by the ATO in respect of standards of authentication and the elevated risk of 'phishing'[1]. APRA has also identified additional prudential concerns with such approaches as outlined below.

[1] Some RSE licensee marketing campaigns observed by APRA to date appear indistinguishable from campaigns by criminal organisations where unsolicited emails and/or fake websites are used in order to deceive individuals into disclosing confidential personal information, including user names and PINs/passwords. This is commonly known as "phishing".

In APRA's view, sending bulk unsolicited communications requesting members to enter personal data undermines the efforts made by financial institutions and the Australian Government to educate the public on safe online behaviour. APRA supports the ATO's emphasis on information security, including industry transition to two factor authentication.

Bulk provision of sensitive member data to third parties

It has become apparent that some RSE licensees, in order to facilitate the practices referred to above, are providing bulk extracts of sensitive member data, including individual tax file numbers (TFNs), to third party service providers. APRA has noted that sensitive member data has also been provided to third parties for other purposes such as business intelligence, customer analytics and marketing.

APRA would like to remind RSE licensees of the risks inherent in such initiatives, including the outsourcing elements within them. RSE licensees are expected to maintain the usual rigour associated with outsourcing and risk management frameworks, and ensure that boards and senior management are fully informed and engaged in appropriate oversight of these arrangements. Boards and management should also ensure they have, or have access to, appropriate expertise to identify and manage current and emerging risks arising from these activities.

Heightened risk

APRA emphasises the need for proper risk and governance processes with respect to the confidentiality and integrity of sensitive member data. APRA considers that bulk extraction of sensitive member data from core administration systems, particularly to environments where security controls are weaker or unproven, gives rise to heightened risk. This applies equally to in-house and outsourced environments.

RSE licensees are encouraged to consult with APRA in the early stages of considering such initiatives. To facilitate consultation, RSE licensees could provide documentation used to inform their risk management and decision-making processes. Whether involving shared computing services or otherwise, guidance can be obtained under the Governance section of APRA's Information Paper on Outsourcing Involving Shared Computing Services.

APRA's prudential framework and the duty to protect beneficial interests

APRA supports industry initiatives to consolidate lost and inactive member accounts, as well as wider objectives of using technology to engage with members, deliver services and improve the administration function. However, prudent practices must be in place and risks adequately mitigated when regulated entities undertake these initiatives.

RSE licensees are also reminded of their responsibility to promote the financial interests of superannuation members and to ensure that members' interests and data are not compromised.

The principles in the following APRA publications are pertinent to the concerns raised in this letter:

- Superannuation Prudential Standard SPS 220 - Risk Management;
- Superannuation Prudential Standard SPS 231 - Outsourcing;
- Prudential Practice Guide CPG 234 - Management of security risk in information and information technology;
- Prudential Practice Guide CPG 235 - Managing data risk; and
- Information Paper on Outsourcing Involving Shared Computing Services.

As part of its regular onsite review processes, APRA will continue to examine outsourcing and other initiatives of regulated institutions to ensure risks are appropriately understood and managed.

Should you have any questions or comments, please contact your responsible supervisor.

Regards

Helen Rowell