Super Consumers Australia

Phone 02 9577 3333
Email enquiries@superconsumers.com.au
Website www.superconsumers.com.au
57 Carrington Road,
Marrickville NSW 2204
ACN 163 636 566 | **ABN** 34 163 636 566

General Manager
Policy
APRA

13 May 2024

RE: Consultation on financial resources for risk events in superannuation – Operational risk financial requirement (ORFR)

The Operational Risk Financial Requirement (ORFR) serves as a crucial financial buffer for super funds to access when covering costs that arise from operational risks. We support APRA's approach simplifying and clarifying ORFR rules, and encourage APRA to surveil and take action against industry members where deficient approaches to the ORFR are identified. Ensuring that the ORFR is fit for purpose is paramount to maintaining the stability and integrity of the super system more broadly.

However, there is a significant and growing risk that the superannuation industry is not ready to address, and it is putting the retirement savings of all Australians at risk, with some already having their savings wiped out.[1] This is the risk of superannuation scams and fraud.

There are many recent examples where super fund members have lost savings due to inadequate or failed fund account security systems and processes, but have often not been reimbursed by the fund. These include instances where a fund failed to:

- Have two-factor authentication for risky transactions in place,[2] [3] [4]
- Check the legitimacy of changes to bank account details,[5]
- Query suspicious transactions,[6]
- Use the correct contact details to verify a member's identity,[7]
- Identify fraudulent documentation.[8]

---

[1] Super Consumers Australia 2024, *Scams – Mandatory Industry Scams code submission*, p. 1-2 https://superconsumers.com.au/wp-content/uploads/2024/03/SuperConsumersSubmissiononScams%E2%80%93MandatoryIndustryCodeconsultation.pdf
[2] AFCA Determination 907631, https://service02.afca.org.au/CaseFiles/FOSSIC/907631.pdf
[3] AFCA Determination 826592, https://service02.afca.org.au/CaseFiles/FOSSIC/826592.pdf
[4] AFCA Determination 806447, https://service02.afca.org.au/CaseFiles/FOSSIC/806447.pdf
[5] AFCA Determination 907631, op. cit.
[6] AFCA Determination 768952, https://service02.afca.org.au/CaseFiles/FOSSIC/768952.pdf
[7] AFCA Determination 672114, https://service02.afca.org.au/CaseFiles/FOSSIC/672114.pdf
[8] AFCA Determination 768952, op. cit.

Additionally, since 2022, up to 178,000 superannuation members have been placed at heightened risk of phishing scams due to known super fund data breaches.[9] [10] [11] Data breaches can lead to an increased risk of phishing scams because scammers can use stolen personal information to target those who have been affected by the breach.

In all but one of the AFCA cases referred to above, AFCA could not make a determination in the member's favour because in its view, the fund had not broken any rules – rules that APRA has a role in establishing through its prudential standards. AFCA determinations on this issue are the clearest indication that:

1. There is a fundamental mismatch between members' expectations of their fund's account security settings and their fund's ability to meet those expectations, and
2. Current policy settings are not adequately protecting people from the risk of super scams and fraud.
3. Even though the ORFR exists, it is not always being used to compensate members who are victims of fraud.

Despite APRA's direction to licensees in 2023 to review their use of multi-factor authentication (MFA),[12] we know MFA is inconsistently applied across the super industry and across communication channels. We are calling on APRA to urgently introduce minimum account security standards for super funds, including two-factor authentication for medium risk transactions, and identification for high risk transactions. It is important these standards remain flexible for members who can't offer traditional forms of ID or meet two-factor authentication requirements. This includes those represented by a financial counsellor or other advocates as is standard in other industries like banking.

Please reach out to Policy Manager [redacted] at [redacted] if you wish to discuss our comments further.

[9] IT News 2022, 50k customers caught up in Spirit Super phishing attack, https://www.itnews.com.au/news/50k-customers-caught-up-in-spirit-super-phishing-attack-580647 50,000 members were affected.
[10] NGS Super, Cyber incident update, https://www.ngssuper.com.au/articles/news/cyber-incident-update NGS Super did not report the number of members affected, but had 114,490 members as of June 2023.
[11] Super SA, Important information – third-party provider cyber security incident,https://www.supersa.sa.gov.au/about-us/announcements/2023/external-provider-cyber-security-incident 14,011 members were affected.
[12] APRA 2023, *Use of multi-factor authentication (MFA)*, https://www.apra.gov.au/use-of-multi-factor-authentication-mfa

Sincerely,

[redacted]

[redacted]
Director, Super Consumers Australia