FSC Standard No. 29

Fraud and Scam Mitigation Measures for Superannuation Funds

1 July 2024

FSC FINANCIAL SERVICES COUNCIL

FSC Standard No. 29

Fraud and Scam Mitigation Measures for Superannuation Funds

18 June 2024

FSC Membership this Standard is most relevant to:	This Standard applies to FSC superannuation members who are trustees (relevant licensees) holding a public offer or extended public offer licence) to operate a Registrable Superannuation entity under the provisions of the Superannuation Industry (Supervision) Act 1993.
Date of this version (and commencement):	This Standard will commence on 1 July 2024 subject to a twenty four (24)-month transition period. This Standard is mandatory for FSC Full Members from 1 July 2026. Earlier compliance is encouraged. There are no previous versions.
Main Purposes of this Standard:	This Standard covers superannuation funds' fraud and scam mitigation measures including the creation of mitigation policies and protective measures on high-risk transactions.
Disclaimer	*This document does not constitute any legal, accounting, tax or financial product advice, and does not take into account the objectives, financial situation or needs of any person or the terms of any commercial transaction. Users should obtain their own professional advice tailored to their own circumstances before using this document for their own commercial purposes. The Financial Services Council Ltd (FSC) does not give any warranty with respect to this document and has no responsibility for any loss, damage or liability whatsoever arising from the use of this document. The use of this document is subject to the terms and conditions prescribed by the FSC from time to time in relation to the access, use, transmission or dissemination of this document*

FSC Standard No. 29

Table of Contents

FSC Standard No. 29

1. Introduction

1.1 This Standard may be cited as FSC Standard No 29: Fraud and Scam Mitigation Measures for Superannuation Funds.

1.2 This Standard covers superannuation fund's fraud and scam mitigation measures including the creation of mitigation policies and protective measures on high-risk transactions.

1.3 This Standard was issued on 18 June 2024.

1.4 Effective Date: this Standard commences operation on 1 July 2024 on a voluntary compliance basis. Full compliance with this Standard takes effect from 1 July 2026 and is mandatory. Earlier compliance with this Standard is nonetheless permitted and encouraged.

1.5 Although mandatory compliance commences from 1 July 2026, the FSC strongly encourages members to make concerted efforts to be as compliant as possible, as early as possible from the commencement of voluntary compliance.

1.6 Application General Principle: this Standard applies to FSC superannuation members who are trustees (relevant licensees) holding a public offer or extended public offer licence (relevant licence) to operate a Registrable Superannuation Entity under the provisions of the *Superannuation Industry (Supervision) Act 1993*.

1.7 Complying with a relevant FSC standard is mandatory as a minimum standard. Trustees may choose to implement processes and standards that further improve customer outcomes.

1.8 This Standard seeks to avoid duplicating any relevant legislation. However, it should be recognised that there may be additional standards set by legislative instruments relevant to fraud and scam mitigation and customer service[1]. Where they may overlap or be inconsistent with this Standard the applicable law or regulation prevails.

1.9 This Standard also does not attempt to prescribe how obligations imposed by legislation or regulatory work in practice. Superannuation funds should ensure that they are complying with all relevant legislation[2], regulation, prudential regulation, and appropriate ASIC rules.

1.10 Nothing in this Standard obliges superannuation funds to resolve complaints relating to Fraud and Scams through the provision of reimbursing losses or any other forms of compensation.

2. Definitions

2.1 Board

Board means either or both of the Board of Trustees and/or the Board of the organisation, as relevant and appropriate.

2.2 Customer

Customer means a customer of the superannuation fund where such fund is a member of the Financial Services Council.

2.3 Fraud

Fraud means any action that involves dishonestly obtaining a benefit, or causing a loss, by deception or other means. It includes theft.

2.4 High-Risk Transactions

High-Risk transactions are as defined in Section 4 of this Standard.

[1] See also ASIC Regulatory Guide RG271: internal dispute resolution and APRA Prudential Standard CPS 234: Information Security.
[2] This also includes obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*

2.5 Multi-factor authentication (MFA)

Multi-factor authentication is a security measure requiring a combination of at least two of the following authentication factors:

- Something that is known to the person (knowledge): a secret the user knows, like a PIN or password.
- Something that the person has (possession): something the user has in their possession, like a hardware or software token or an SMS text message.
- Something that the person is (inheritance): something rooted in the user, like a biometric identifier, such as a fingerprint or facial recognition.

Other factors, such as location, may be relevant.

In combination, these authentication factors ensure that the only person who is authenticated is the legitimate user, even if other pieces of data have been collected or stolen.

2.6 Scam

Scam means any action where a person has been illegally tricked or deceived into handing over money or personal details.

2.7 Senior Executives

Senior Executives means the Senior Executives who take part in the management of the organisation and/or superannuation fund, as relevant and appropriate.

2.8 Staging Account

An account created for the purpose of consolidating or transiting through fraudulently obtained funds before they are further transferred or withdrawn from the superannuation system.

2.9 Trustee (Board of Trustees)

The person(s) or organisation who manages the superannuation fund, scheme or trust.

2.10 Vulnerable Persons

Vulnerable persons means either a child or children, or an individual aged 18 years and above who is, or may be, unable to take care of themselves, or is unable to protect themselves against harm or exploitation by reason of age, illness, trauma or disability, or for any other reason.

3. Scam and Fraud Mitigation Measures

3.1 Internal Policies for Scam and Fraud Mitigation

3.1.1 Trustees should ensure that their customers are protected from the harms of scam and fraud using means that are reasonable and proportionate to the size and structure of the business and in so far as is practicable and within the Trustee's control.

3.1.2 Superannuation funds should have an organisational policy for the purpose of dealing with scams and fraud events including:

- The prevention of fraud and scam events.
- The approach to detecting and disrupting fraud and scam events including training of relevant staff.
- How the organisation will respond to the fraud and scam event including how it will interact and communicate with its customers.
- How the organisation intends to monitor compliance with, implement, and review the scams and fraud policy to ensure that it remains relevant.

- How the organisation intends to manage the risks associated with vulnerable customers, including but not limited to the elderly and those from culturally and linguistically diverse CALD backgrounds.

3.1.3 For the purposes of clause 3.1.2, this policy could be contained or exist with reference to multiple existing policies within the organisation.

3.1.4 Where appropriate this strategy should be organisation wide and should carefully consider the specific needs of superannuation customers.

3.1.5 Any scam and fraud mitigation and resolution policies must have regard to customer outcomes and experience.

3.2 Oversight and Responsibilities

3.2.1 Organisations should have a clear understanding of who is responsible for the various parts of implementation of the scams and fraud mitigation policy, including who within the organisation is responsible for ensuring resolution of scam and fraud matters for customers.

3.2.2 Where appropriate, the superannuation fund should report relevant superannuation fraud and scam statistics and information to relevant Senior Executives and its Board. Relevant statistics and information may include:

- The number of fraud and scam incidents within the given period.
- Resolutions and outcomes.
- Relevant metrics relating to the customer experience.
- Relevant scams threat environment information.
- Any systemic issues identified.

4. High Risk Transactions

4.1 Fraud and Scam Mitigation for High-Risk Transactions

4.1.1 Superannuation funds must have in place, mitigation measures for the management of high-risk transactions.

4.1.2 Mitigation measures should be relevant to the size, structure, and complexity of the organisation.

4.1.3 This includes, but is not limited to, the use of multi-factor authentication measures (where applicable) or an appropriate alternative where multi-factor authentication is not suitable.

4.2 Alternatives To Multi-Factor Authentication

4.2.1 Where a superannuation fund determines multi-factor authentication is not appropriate, alternatives to multi-factor authentication may include but are not limited to:

- Biometric Authentication: biometric authentication adds an extra layer of security to logins and verifies users' identities through physical characteristics. These could include fingerprint scanners, voice recognition, facial recognition, and even retinal scans.
- One Time Passwords: one-time passwords (OTPs) are single-use codes used to confirm a user's identity. The OTP is sent to the user's phone through SMS, software application, or email and is only valid for a limited period of time.
- Security Questions: security questions provide another layer of security when logging into online accounts. These questions usually require information that only the actual user would know, such as where they grew up or their mother's maiden name.
- Electronic Identification (EID, through the Document Verification Service).

4.3 High-risk transactions

4.3.1 For the purposes of this Standard, high-risk transactions for which multi-factor authentication, or an appropriate alternative should be utilised, where appropriate, are taken to be:

- Any transaction which involves the amendment of key contact details including name, date of birth, phone numbers, or email addresses.
- Any transaction which involves the amendment of bank account details, including BSB and/or account number.

4.3.2 For the purposes of this Standard, high-risk transactions for which other appropriate mitigation measures, such as monitoring and deeper scrutiny should be utilised, where appropriate, are taken to be:

- Any transaction or behaviour which, in the Trustee's opinion indicates the account may be being used as a staging account for fraudulent behaviour.
- Any transaction which, in the opinion of the Trustee, may be cause for further scrutiny, including, but not limited to signs of elder or vulnerable person abuse, unexplained wealth or unusually large or irregular contributions inconsistent with the customer's existing profile.

4.4 Opting out of Multi-Factor Authentication

4.4.1 Superannuation funds have the discretion to allow customers to opt out of multi-factor authentication in cases where, in the superannuation fund's opinion, the use of multi-factor authentication is unduly onerous. Cases where it may be unduly onerous include, but are not limited to:

- Instances where a person does not have the means to enact MFA for example, lacking in reliable phone service or a low level of skill with mobile phone technology, making it difficult for them to respond to an MFA request in a timely manner.
- Instances where a person does not have access to traditional forms of ID that prevent them from accessing the means to enact MFA.

4.4.2 In instances where a person does not have the means to enact MFA, other measures of proving identity must be considered for protection of that person's account.

4.4.3 Customers should be informed of the risks of removing such protective measures from their accounts - see Clause 5.4 below.

4.4.4 If a customer has opted out of multi-factor authentication, superannuation funds should continue to maintain other relevant mitigation measures on that customer's account as per this Standard.

4.4.5 If a customer wishes to add multi-factor authentication back onto their account, it should be easy for them to do so.

5. Communicating with Customers

5.1 Superannuation funds should ensure that their customers are aware of existing policies that relate to the resolution of customer complaints as they relate to both internal and external dispute resolution forums.

5.2 If there are delays to transactions and/or other actions on an account as a result of fraud and scam mitigation measures, in so far as is reasonable and compliant with relevant legislation, superannuation funds should communication with the relevant customer concerning the reasons for the delay.

5.3 Superannuation funds should communicate with their customers the importance of multi-factor authentication and other scam and fraud mitigation measures, including any alternative measures in place where the customer is unable to utilise multi-factor authentication.

5.4 If a superannuation fund customer has opted out of a fraud and scam mitigation measure, such as multi-factor authentication, this should be clearly and directly communicated to the customer, including the potential consequences of not having protective measures on their account.

5.5 Superannuation funds should actively encourage customers to be scam and fraud aware and protect themselves from the risk of exploitation for scam and fraud purposes by choosing secure passwords and keeping their important personal information safe.

6. Useful Resources

Australian Competition and Consumer Commission:
https://www.accc.gov.au/consumers/protecting-yourself/scams

Cyber Protect:
https://www.cyber.gov.au/protect-yourself/resources-protect-yourself/personal-security-guides/protect-yourself-multi-factor-authentication

eSafety Commissioner:
https://www.esafety.gov.au/key-topics/staying-safe/online-scams

Money Smart:
https://moneysmart.gov.au/check-and-report-scams/what-to-do-if-you-ve-been-scammed

National Anti-Scam Centre:
https://www.scamwatch.gov.au/

Services Australia (resources for Community Groups):
https://www.servicesaustralia.gov.au/scams-and-identity-theft-resources-for-community-groups?context=64107