FSC Standard No. 29

Fraud and Scam Mitigation Measures for Superannuation Funds

8 August 2025

FSC FINANCIAL SERVICES COUNCIL

FSC Standard No. 29

Fraud and Scam Mitigation Measures for Superannuation Funds

8 August 2025

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 version of the is effective from 8 August 2025. The mandatory compliance date for the requirements of Section 6.4 of this Standard, as reissued on 8 August 2025, is 31 August 2025 . The mandatory compliance date for the requirements of all other parts of this standard, other than those listed in Clause 3.2.1 of this Standard, as re-issued on 8 August 2025, is 1 July 2026 .
Previous version:	1 July 2024
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 Standard Application

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

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

1.1.3 This Standard was originally issued on 18 June 2024 and this version was issued on 8 August 2025.

1.1.4 Application General Principle: this Standard applies to FSC Full 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.

1.1.5 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.

1.1.6 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.

1.1.7 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.

1.1.8 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

Board

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

Customer

Customer means a customer of the superannuation fund, sometimes referred to as a member, where such fund is a member of the Financial Services Council. Customer may also mean the beneficiary of a superannuation fund customer or their authorised representatives, as appropriate.

Fraud

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

High-Risk Transactions

High-Risk transactions are as defined in Section 6 of this Standard.

Person Experiencing Vulnerability

A person experiencing vulnerability is an individual who faces an increased risk of harm, exploitation or isolation. This can be due to various factors including, but not limited to, social, economic, physical or mental

[1] See Appendix D for a full list of relevant legislative and regulatory matters.

[2] This also includes obligations under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006.

health conditions, disability, age, lack of access to essential services, or other personal circumstances. More information about vulnerability is contained in Section 6.9.

Scam

Scam means a direct or indirect attempt (whether successful or not) to engage a consumer in a way that it would be reasonable to conclude would, if successful, cause loss or harm.

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.

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.

Trustee (Board of Trustees)

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

3. Scope and Commencement

3.1 Scope of Standard

3.1.1 This Standard applies to all FSC member superannuation trustees who are full members of the FSC.

3.1.2 Throughout the Standard there is also “Implementation and Best Practice Guidance” which is intended to provide more fulsome guidance for implementation and help steer industry towards best practice but is not compulsory.

3.1.3 Although the best practice guidance is not compulsory, the FSC expects funds to adopt a culture of continuous improvement and continue to work towards implementation of best practice solutions, as relevant to the size, scale, and customer base of the individual fund.

3.2 Commencement

3.2.1 The mandatory compliance date for the requirements of Section 6.4 of this Standard, as re-issued on 8 August 2025, is 31 August 2025.

3.2.2 The mandatory compliance date for the requirements of all other parts of this standard, other than those listed in Clause 3.2.1 of this Standard, as re-issued on 8 August 2025, is 1 July 2026.

3.3 Attestation of Compliance

3.3.1 As per FSC Standard No 1: Code of Ethics and Code of Conduct; FSC Full Members must submit to the FSC, a statement as to their compliance with relevant Standards each year.

3.3.2 Where a fund is not in a position to comply with the commencement of mandatory compliance of Section 6.4 of this Standard from 31 August 2025, they must submit, with their annual attestation, an explanation as to why the fund does not comply, along with an explanation of expected remediation, including a date of expected compliance.

3.3.3 The FSC may, from time to time, conduct reasonable enquiries to determine compliance with this Standard, which may involve the use of independent third parties. Any such review will maintain strict confidentiality and reporting will be conducted on an anonymous basis. The FSC expects that FSC members will co-operate with any such enquiry.

3.3.4 Following the commencement of this Standard from 8 August 2025, for compulsory compliance with Clause 6.4 the first period of attestation will be for the period 31 August 2025 until 30 June 2026. This attestation collection process will commence from 1 July 2026.

3.3.5 For all other parts of the Standard, the first period of attestation will be for the period 31 August 2026 until 30 June 2027. This attestation process will commence from 1 July 2027.

4. Fraud and Scam Mitigation Measures

4.1 Fraud and Scam Mitigation Measures

4.1.1 Throughout this Standard, the FSC refers to "measures". In most instances the specifics of these measures are not defined but should be reasonable and proportionate to the size and structure of the business and in so far as is practicable and within the Trustee's control.

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

4.2 Internal Policies for Fraud and Scam Mitigation

4.2.1 Superannuation funds should have an organisational policy outlining the fund's approach to preventing, detecting, and disrupting fraud and scams. This organisational policy should include:

- 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 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 fraud and scams policy to ensure that it remains relevant.
- The metrics by which the fund intends to measure the effectiveness of its fraud and scam mitigation measures, and, where appropriate, any targets the fund has for reducing fraud and scam incidents.
- How the organisation intends to manage the risks associated with persons experiencing vulnerability (see Section 6.9 below).

4.2.2 For the purposes of clause 4.2.1 this policy could be contained or exist with reference to multiple existing policies within the organisation but should nonetheless be clear to those that must rely on it.

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

4.2.4 Any fraud and scam mitigation and resolution policies should have regard to customer experience to ensure customer outcomes remain paramount.

Implementation and Best Practice Guidance

- Fraud and scam prevention policies should be tailored to the organisation.
- A suggested outline is included in Appendix B for funds to reference.
- Although the fraud and scam policy(ies) are likely to be highly confidential, funds should consider how it can communicate key parts of the policy to its customers.

5. Obligations Relating to Fraud and Scam Incidents

5.1 Detecting and Preventing Fraud and Scam Incidents

5.1.1 Funds should have in place measures which allow it to adequately and reasonably prevent and detect fraud and scam behaviours.

5.1.2 Funds must have in place the measures outlined in Section 6 relating to high-risk transactions.

5.1.3 For the avoidance of doubt, funds should also have in place a framework for detecting and preventing fraud and scams on other transactions not outlined in Section 6 including:

5.1.3.1 Any transaction or behaviour which, in the reasonable opinion of the Fund, indicates the account may be being used as a staging account for fraudulent behaviour.

5.1.3.2 Any transaction which, in the reasonable opinion of the Fund, may be cause for further scrutiny, including, but not limited to, signs of elder or vulnerable person abuse.

Implementation and Best Practice Guidance

- Measures for preventing scams include, but are not limited to:
  - Proactive education for customers about what to look for with regard to scam behaviour.
  - Proactive education of frontline staff to help identify where a customer may be subject to a scam.
    - ⇒ Red flags for scam-initiated behaviour include but are not limited to:
      - ♦ A customer wanting to make an urgent transaction. It is important to note that in the superannuation environment, investment decisions can have a short time horizon or natural urgency, and this in and of itself is not a red flag, however, context is important. For example, a customer being urged to make a quick decision may warrant further consideration.
      - ♦ Cold calls or unsolicited contact claiming to be from official or benevolent sources such as the government, bank, fund, financial advisers.
      - ♦ Promises of unrealistic returns.
      - ♦ Complex or poorly disclosed information.
      - ♦ Limited or no face-to-face contact with another party urging the transaction.
  - Proactive communications during and after high-risk transactions occur to encourage the customer to contemplate whether the transaction may be part of a scam.
    - ⇒ For example, a customer may be asked or prompted to consider their circumstances with the following questions:
      - ♦ Did you initiate this transaction yourself?
      - ♦ Do you know the person or business you are sending money to/investing with?
      - ♦ How did you come into contact with this person or organisation?
      - ♦ What is the purpose of this payment?
      - ♦ Have you been asked to keep this transaction secret?
      - ♦ Has anyone pressured you to make this payment urgently?
      - ♦ Were you contacted unexpectedly by someone claiming to be from the fund, a bank, government agency, or tech support?
      - ♦ Did you receive a message or call asking you to move your money to a “safe account”?
      - ♦ Have you been told your account has been compromised and you need to act quickly?
- Measures for preventing fraud include, but are not limited to:

- Proactive education for customers about the importance of protecting themselves from the risks of identity theft.
- Implementing an identity authentication regime (noting the requirements of Section 6 of this Standard).

- Measures for detecting fraud and scam activity include, but are not limited to:
  - Investigating, in a timely manner, activities that are the subject of actionable scam intelligence
    - ⇒ Actionable scam intelligence means there are reasonable grounds for the fund to suspect that a communication, transaction or other activity is a fraud or scam. Whether there are reasonable grounds for such a suspicion is an objective test, relevant information for this test may include:
      - ♦ information about the mechanism or identifier being used, such as URLs, email addresses, phone numbers, social media profiles, digital wallets and bank account information of the suspected perpetrator.
      - ♦ information about the suspected perpetrator.
      - ♦ information (including complaints) provided by customers.
  - Identifying, in a timely manner, if there is potential for other customers of the fund to have been impacted by known scam and fraud events and activities, for example if the scammer has used credential stuffing to access multiple accounts.
  - Creating a framework through which transactions can be assessed as to whether they are likely to be related to fraud and scam. This might be done through manual transaction monitoring or with the help of software solutions, or a combination of both.
  - Conducting, whether based on the framework noted above, or another risk-based framework, withdrawal checks to confirm why money is being withdrawn.

5.2 Customers Who Have Been Affected by Fraud and Scam Activity

5.2.1 Funds should have in place easy mechanisms for customers to report potential fraud and scam activity.

5.2.2 Reports of fraud and scam activity should be dealt with in a timely manner.

5.2.3 Nothing in this Standard affects the fund's regulatory requirement to give effect to rollover requests within the regulated maximum time frames.

Implementation and Best Practice Guidance

- Funds should carefully balance the need to prevent fraud and scam transactions with the interest of a genuine customer attempting a genuine transaction. What is a reasonable maximum timeframe for processing transactions, in addition to the regulated service level agreement, is determined by risk factors including the size and scale of the transaction, previous customer behaviours, and whether the transaction genuinely appears to be either fraudulent or a scam.

5.3 Oversight and Responsibilities

5.3.1 Organisations should have a clear understanding of who is responsible for the various parts of implementation of the fraud and scams mitigation policy as per Section 4.2, including who within the organisation is responsible for ensuring resolution of fraud and scam matters for customers.

5.3.2 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 fraud and scams threat environment information.
- Any systemic issues identified.
- Any associated management action plans to address arising and systemic issues.

5.4 Information Sharing Capabilities

5.4.1 Subject to privacy, security, and other legislative concerns, superannuation funds should contribute to a culture of collaboration with regard to protecting Australians from the threats of fraud and scams.

5.4.2 Funds should avail themselves of opportunities to share information in appropriate and secure forums.

5.4.3 Subject to privacy, security, and other legislative concerns, both during and after an incident, funds should act in the interests of both their customers and the wider superannuation ecosystem to ensure that relevant and timely information is shared for the purpose of assisting other entities to manage threats.

Implementation and Best Practice Guidance

- There are two forms of information that are useful to be shared about fraud and scam activity, qualitative information about threats and emerging issues, and data such as known scam phone numbers and bank account details.
- Funds looking to implement best practice should find ways to be involved in both forms of information sharing.
- The FSC hosts regular qualitative information sharing forums focussed on cybersecurity and fraud/scams respectively. These forums are open to all superannuation funds, regardless of FSC membership status. For more information on these forums please contact info@fsc.org.au.

5.5 Review of Fraud and Scam Mitigation Measures

5.5.1 Funds should have in place a framework for reviewing the measures contained in all aspects of operations required in this Standard to ensure that they are working effectively and remain relevant as per clause 3.1.3.

6. Specific Measures for Mitigating Fraud on High-Risk Transactions

6.1 Authentication for High-Risk Transactions

6.1.1 Superannuation funds must have in place authentication measures for the management of high-risk transactions, the definition of which is outlined in clause 6.2.1.

6.1.2 Authentication measures should be relevant to the particular channel in which the fund is interacting with the customer. Expectations for each channel are outlined in the following sections.

6.1.3 If a customer provides a reasonable explanation as to why they cannot authenticate themselves using a particular method, the fund should work with the customer to identify an appropriate alternative authentication method. More information about this obligation can be found in Section 6.8 and Clause 6.4.5.

6.1.4 For the avoidance of doubt, authentication is a measure used to prevent fraud and is not necessarily a useful tool in preventing scams. Further, it is only one tool in a suite that can be used to prevent and mitigate fraud. Therefore, funds should employ a multi-layered approach with measures that are targeted at fraud, scams, and both fraud and scams.

6.2 High Risk Transactions

6.2.1 For the purposes of this Standard, the following transactions are considered high-risk:

a. Any transaction which involves the amendment of key contact details including name, date of birth, phone numbers, residential address, or email addresses.
b. Any transaction which involves the amendment of bank account details, including BSB and/or account number.
c. Any transaction which involves withdrawing funds either:
   i. In the case of an account-based pension, for the initial set up of the payment; or
   ii. In the case of lump sum and/or ad-hoc withdrawals, for each transaction of this type.
d. Any transaction which involves a rollover request of funds from one APRA regulated entity to either another APRA regulated fund or a Self-Managed Superannuation Fund that is initiated within the fund's environment and control.[3]

6.3 Authentication Measures by Channel

6.3.1 For the purposes of this section, the requirements apply whether or not the transactions are conducted by the customer themselves or through an intermediary using privileged or administrator access. This includes where accounts are being accessed by financial advisers on behalf of a customer but not for transactions conducted through the ATO MyGov portal, including rollover requests and payments made in accordance with release authorities (see footnote 3).

6.4 Digital/Web Based Channels

6.4.1 Digital and web-based channels are those which are conducted over the internet using a digital device such as a computer or mobile phone. These transactions are often, but not always, completed by the customer without the assistance of the fund or another intermediary, as distinguished from non-digital/web based transactions outlined in later sections. They include, but are not limited to transactions that are conducted through the fund's official customer portal, or app.

6.4.2 Digital and web-based channels should have a form of identity verification authentication when conducting high-risk transactions. See the Best Practice Guide below for information about authentication options.

6.4.3 For the avoidance of doubt, if a fund has authentication on log in to an account, but not for specific transactions conducted thereafter, this will satisfy the requirements of Clause 6.4.2 however, the fund should note the Implementation and Best Practice Guidance advice contained below.

Implementation and Best Practice Guidance

- Although it is noted that the authentication requirements in this Standard are satisfied when conducted either at account log in, or when conducting the high-risk transaction itself, funds should work towards having step up authentication, which would allow for authentication both at log-in and again when a high-risk transaction is attempted.

Multi-Factor Authentication

- Multi-factor authentication (MFA is a security measure requiring a combination of at least two of the following authentication factors:
  - Something that is known to the person (knowledge) such as a secret the user knows, like a PIN or password.

[3] For clarity, some rollover requests are initiated through the ATO MyGov environment, there is no expectation that funds conduct multi-factor authentication on these types of transactions.

- Something that the person has (possession): such as something the user has in their possession, like a hardware or software token or an SMS text message.
- Something that the person is (inheritance) such as something rooted in the user like a biometric identifier (fingerprint or facial recognition).
- Other factors such as location, may be relevant.

- In combination, these authentication factors can help to ensure that the only person who is authenticated is the legitimate user.
- There are varying forms of multi-factor authentication available to funds, all with varying levels of security. At the time of publishing this Standard, the following forms of MFA should be considered by funds in dispensing their obligations:
  - **Passkeys** (very high security) – a passwordless login method using cryptographic keys stored on an individual's device, verified via biometrics or device PIN; highly secure and phishing-resistant.
  - **Smartcards/digital certificates** (very high security) – identity verification through a card or file containing a digital certificate, often with PIN protection.
  - **Authenticator apps** (high security) – smartphone apps like Google Authenticator or Okta that generate time-based one-time passcodes (TOTP) every 30 seconds and is not reliant on mobile networks and more secure than SMS.
  - **Push notification authentication** (high security) – a login request is sent to an individual's mobile device and that individual must tap "approve" to confirm; this may be vulnerable to approval fatigue meaning a person does not register what they are approving.
  - **Biometric authentication** (high security) – uses fingerprint, facial recognition, or voice to verify an individual's identity.
  - **SMS one-time passcodes** (moderate security) – a code is sent to an individual's phone by text message after password entry; can be vulnerable to SIM swapping and interception.
  - **Email one-time passcodes** (moderate security) – a code is sent to an individual's email inbox after password entry. This can be less secure due to risk of compromised email accounts.
- When utilising the One-Time Password/Passcode options, funds should carefully consider the content of the passcode message to ensure it, where possible, outlines the risks of sharing the passcode.
- When implementing MFA, or a new type of MFA for the first time, funds should take all reasonable steps to ensure that the MFA reaches near universal take-up as quickly as possible. This includes proactively ensuring MFA is switched on, rather than waiting for a customer to switch it on.

6.4.4 Opting out of Authentication

6.4.4.1 Superannuation funds have the discretion to allow customers to opt out of authentication in cases where, in the superannuation fund's opinion, the use of authentication is unduly onerous or the customer is experiencing a vulnerability that precludes them from enacting authentication controls (either as a one-off, or on ongoing basis).

6.4.4.2 As per Clause 6.1.3 funds should work with customers who are affected under Clause 6.4.4.1 to provide alternative solutions.

6.4.4.3 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 may prevent them from authenticating themselves.

- Cases of vulnerability as outlined in (but not limited to) Section 6.9.

6.4.4.4 Customers should be informed of the risks of removing such protective measures from their accounts - see Section 7 below.

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

6.5 Paper Based Channels

6.5.1 Paper based channels are those that require a person to complete a paper based form and submit this via mail, in person, or other means, directly to the fund to affect a transaction.

6.5.2 Funds should have in place measures to verify the authenticity of requests received using this channel.

Implementation and Best Practice Guidance

- Verification of paper-based processes include but are not limited to:
  - Requiring the provision of certified identity verification documents.
  - Requiring bank statements also be provided when changing bank details.
  - Having a follow up contact with the customer via voice or in person, to confirm the request.
  - Handwriting or signature verification.
- When verifying identification, funds should also have reference to concerns around collecting and storing sensitive data. ID verification services can help to mitigate these risks.

6.6 Non-Digital Direct Transactions

6.6.1 Non-digital direct channels are those where a customer must interact with the fund to affect the transaction. This includes where a customer has contacted the fund directly to make changes to their account.

6.6.2 Funds should have in place measures to verify the identity of the customer before completing any high-risk transaction requests on this channel.

Implementation and Best Practice Guidance

- Measures that can be used to verify a customer over the phone include but are not limited to:
  - Pre call risk assessment:
    - ⇒ Checking caller ID against customer records.
    - ⇒ Using call history and previous flags for vulnerability or previous fraud attempts.
    - ⇒ If suspicious behaviour is noted, consider alternative channels or callback on verified numbers.
  - Multi-layered identity verification of at least two different/independent (i.e. not found from the same source) identity factors such as:
    - ⇒ Full name and date of birth.
    - ⇒ Customer number or unique fund identifier.
    - ⇒ Recent contribution amount or transaction history verification including:
      - ♦ Registered address.
      - ♦ Employer details (based on contribution history).
    - ⇒ Knowledge based authentication using dynamic, hard to guess/research questions:
      - ♦ “Can you confirm the date and amount of your last contribution?”
      - ♦ “What is the name of your current employer?”
      - ♦ “Which beneficiary have you most recently nominated?”
    - ⇒ Out-of-Band Verification:

- ♦ When possible, conduct a callback to a pre-registered phone number or send a one-time passcode to the customer's registered email or mobile.
- ♦ Confirm the transaction details during callback.

- Customers experiencing vulnerability may require extra assistance with verification. More information about assisting customers experiencing vulnerability to verify themselves is contained in Section 6.9.
- Verification over the phone should be logged for future reference:
  - Log all identity verification steps, questions asked, and customer responses.
  - Record the date/time and staff member handling the call.
  - Keep records for audit and dispute resolution.
- Frontline staff should be well across fraud, scam, and suspicious activity protocols which could include:
  - Declining or deferring the request if identity cannot be confidently verified (subject to vulnerability considerations).
  - Escalating suspicious calls to fraud or compliance teams immediately.
  - Following up with the customer to confirm any recent changes.
- Frontline and fraud and compliance teams should receive regular training and updates about fraud and scam activity including:
  - Providing ongoing staff training on evolving fraud tactics and verification best practices.
  - Reviewing call scripts and verification questions regularly.

6.7 Communicating with Customers Following High-Risk Transactions

6.7.1 Following the completion of a high-risk transaction, funds should have in place the ability to contact a customer to alert them to the transaction, if the fund identifies that this is necessary for security purposes.

6.7.2 Funds should elect to use the quickest method available to them that is appropriate for this interaction.

Implementation and Best Practice Guidance

- Funds have a number of options available to them in relation to contacting a customer to confirm high-risk transactions including, but not limited to:
  - SMS message to the mobile service number which is listed on the customer's account (this should not be to an updated mobile number if the high-risk transaction was the changing of the mobile number).
  - Email to an email address that has been validated by the customer previously.
  - An in-app message.
- The message should inform the customer:
  - that a high-risk customer interaction has been initiated; and
  - what the relevant person can do if they did not authorise the interaction.
- Best practice would have the customer's post-transaction contact be on a separate communication channel to that of the authentication that occurred. For example:
  - If the customer requested a transaction via the app and was verified with multi-factor authentication via a text one-time passcode, the confirmation should be sent by email, not SMS.
  - If the customer requested a transaction via the call centre and was verified with an in-app push notification, the confirmation should be sent via SMS, not an in-app push notification.

6.8 Information That Can Be Accessed in Customer Portals

6.8.1 Funds should ensure that, where possible, customer data remains secure behind the customer portal, in the event it is accessed fraudulently. This includes, but is not limited to, ensuring that sensitive customer data such as phone numbers and date of birth are masked in the portal, even when a customer has securely logged in.

6.9 Persons Experiencing Vulnerability

6.9.1 Funds should have in place a policy for dealing with customers who have particular vulnerabilities in relation to the matters contained in this Standard.

6.9.2 Vulnerabilities include, but are not limited to:

- People who are elderly
- People who are minors or otherwise very young
- People from First Nations backgrounds and communities
- People from culturally and linguistically diverse backgrounds including refugees, asylum seekers, and recent migrants to Australia
- People with disabilities
- People who are displaying signs that they may be experiencing some type of coercion, abuse, or family and domestic violence
- People in areas with poor mobile and internet connectivity
- People experiencing mental and physical ill-health including being in a hospital setting for a significant period of time
- People who are experiencing hardship, including financial, emotional, or otherwise including:
    - people who have been recently affected by a natural disaster
    - people experiencing financial hardship
    - people experiencing homelessness, or are, in the fund's reasonable opinion, at risk of experiencing homelessness
    - people recently released from prison

6.9.3 It is noted that not all people in these circumstances are experiencing vulnerability, and these factors should merely be used to assess if the person may be experiencing vulnerability in conjunction with other factors.

6.9.4 A fund's policy, with respect of clause 6.9.1 should outline:

- how the fund generally defines vulnerability
- how the fund approaches flexibility with regard to implementing fraud and scam protections for people who are experiencing vulnerability.

6.9.5 Funds should also have in place a framework for identifying potential vulnerabilities and invest in training front of house staff.

Implementation and Best Practice Guidance

- When interacting with persons experiencing vulnerabilities, it is important that processes be flexible and led with humanity and empathy.
- Policies should be created and informed by lived experience.

Identifying and Managing Vulnerabilities

- Funds should have in place processes to identify and manage vulnerabilities that may arise for customers. This includes:
    - Implement specialist training so frontline and call centre staff can:
        - ⇒ Recognise signs that a customer may be experiencing vulnerability including but not limited to signs of distress, coercion, cognitive decline, or hardship.

⇒ Respond with empathy and patience.

⇒ Know when and how to escalate or refer cases to a specialist team.

⇒ Consider how systems can be used to track known needs, however, consideration should be given to collection and use of sensitive data.

– Watch for red flags of coercion or abuse and respond appropriately.

– Maintain a list of relevant support services and refer customers to the right service to address their needs. Support services include, but are not limited to, 1800RESPECT, IDCARE[4], or financial counselling networks where appropriate.

Authenticating Identity When Vulnerabilities Exist

- When authenticating the identity of a vulnerable person, flexibility might include:
  - For multifactor authentication:
    - ⇒ Allowing secure alternatives for customers who cannot use smartphones, SMS, or email (e.g. postal passcode, voice ID, call-back verification)
    - ⇒ Using voice biometrics or call-based authentication.
    - ⇒ Using larger fonts, simplified instructions, or translated materials for people with disabilities or limited English literacy.
  - Where multi-factor authentication cannot be used:
    - ⇒ Training staff to complete manual verification using secure knowledge-based authentication (e.g. asking previously recorded security questions or details about prior transactions).
    - ⇒ Using paper-based identification by accepting certified copies of ID documents by post or in-person where digital upload is not possible.
    - ⇒ Having policies and frameworks in place that permit an authorised representative, power of attorney, or support worker to assist, where appropriate and safely verified.
- Relaxation of authentication requirements should only occur through a controlled exception process with strong oversight. See Clause 6.4.4 for more information on opting out of MFA.

Example Process – Secure ID verification for a customer experiencing vulnerabilities

- The following is an example process for managing a customer who cannot complete MFA processes due to a vulnerability:

1. Customer calls unable to use SMS MFA.
2. Staff identify possible vulnerability (e.g. elderly, limited tech skills).
3. Offer options:
   - i. Verify via phone using pre-agreed security questions or account-based questions.
   - ii. Send a paper form for completion and ID certification.
   - iii. Allow appointment with a community service to assist.
4. Escalate to customer support team equipped to deal with vulnerabilities for a case note and temporary exemption if needed.
5. In some circumstances it may be appropriate for other follow up actions including referring a customer to financial counselling or, in extreme cases conducting a welfare check.

Inclusive Communications

- Funds should ensure they make all communications inclusive. This includes:
  - Providing relevant instructions (such as setting up and using authentication) in multiple languages, Easy English, and accessible formats (e.g. large print, audio, braille).
  - Ensuring translation and interpreter services are readily available — especially for CALD and Indigenous communities.

[4] Please note that IDCARE is a service that requires a subscription for referral.

- Avoiding jargon — using plain language when explaining ID or security steps.

- Funds should also collaborate with trusted community resources such as:
  - Indigenous Liaison Officers or trusted community organisations.
  - Disability support groups to co-design accessible processes.
  - Financial counsellors who often assist customers with complex needs.

7. Communicating with Customers

7.1 Proactive Communication

7.1.1 Funds should communicate with customers about the importance of protecting themselves and their accounts from the risks for fraud and scam. This includes proactive education campaigns to help customers recognise the signs of fraud and scams.

7.1.2 What is an appropriate cadence of communications should be determined with reference to a risk framework. For example, where there has been a significant increase in scam or fraud activity in recent weeks, the fund may consider it appropriate to push more targeted communications in addition to a regular cadence of marketing emails offering general advice about protections.

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

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

7.1.5 Superannuation funds should ensure that their communications are not unwittingly enabling scammers.

Implementation and Best Practice Guidance

- When communicating with customers generally, funds should have regard to how their communications might be used and spoofed by bad actors. Funds should consider mitigating spoofed scam communication behaviour by:
  - Not sending links in official communications but instead pointing the customer to where on the app or web portal they need to go to transact.
  - Reinforcing messaging that the fund will never request a customer log on via a link or request personal details.

7.1.6 Superannuation funds should ensure that customers experiencing vulnerability have access to education tools that help them navigate fund processes with regard to fraud and scams.

7.1.7 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.

7.2 Complaints Handling

7.2.1 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.

7.2.2 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 communicate with the relevant customer concerning the reasons for the delay.

Implementation and Best Practice Guidance

- When communicating with customers about resolving fraud and scam issues, funds should:
  - Regularly inform customers about how to raise concerns or complaints via multiple channels (website, welcome packs, statements, email).
  - Use plain English to explain the internal dispute resolution process and the role of external dispute resolution bodies like AFCA.
  - Ensure complaint procedures are accessible for people with disabilities, CALD backgrounds, and persons experiencing vulnerabilities (translated materials, large print, etc.).
  - Include contact details and clear timeframes, e.g., “we aim to resolve complaints within 45 days.”

8. APPENDIX A: Useful Resources

Scam, Fraud & Cybersecurity Awareness

- Australian Competition and Consumer Commission (ACCC)
  - ScamWatch (**Link**)
  - Scams Protection for Consumers (**Link**)
- Australian Cyber Security Centre (ACSC) (**Link**)
- Australian Signals Directorate (ASD) MFA & Personal Security Guides (**Link**)
- eSafety Commissioner – Online Scam Protection and Reporting (**Link**)
- ASIC MoneySmart – Scam Response and Consumer Financial Advice (**Link**)

Supporting Persons With Vulnerabilities Customers

- Australian Financial Complaints Authority (AFCA) – Approach to Vulnerable Customer Complainants (**Link**)
- ASIC – Consumer Vulnerability Resources (**Link**)
- Services Australia – Scams and Identity Theft Resources for Community Groups (**Link**)
- IDCARE – National Identity & Cyber Support Service (**Link**)
- Department of Social Services (DSS)
  - Accessibility and Inclusion Toolkit (**Link**)
  - National Plan to End Violence Against Women and Children (**Link**)

Identity Verification, AML/CTF and Risk Management

- AUSTRAC – AML/CTF customer identification and verification (**Link**)
- ATO – Super Stream Identity Verification Standards (**Link**)
- APRA Prudential Standard CPS 234 – Information Security (**Link**)
- APRA – Prudential Practice Guide CPG 234 – Information Security (**Link**)

9. APPENDIX B: Example Fraud and Scam Mitigation Policy Outline

Below is an outline of an example fraud and scam mitigation policy. It has been drafted with the intention that this would be an internal document, not for public distribution. Funds should consider how it can make parts of this policy available to customers so that they can better understand the fund's processes related to fraud and scam mitigation.

1. Purpose

- Outline the organisation's commitment to protecting customers, assets, and data from fraud and scams.
- Align with obligations under the Corporations Act 2001, ASIC Regulatory Guidelines, ACCC Scamwatch, APRA standards, and AUSTRAC reporting requirements.
- Reinforce the need for a proactive, measurable, and inclusive approach to fraud and scam mitigation.

2. Scope

Define the scope of the policy including who it applies to and what kinds of fraud and scam events are captured.

3. Definitions

Provide any relevant definitions.

4. Roles and Responsibilities

Provide an overview of all roles and responsibilities including:

- Board & Executive Leadership
- Risk and Compliance Team
- Fraud Operations or Security Team
- Customer Service & Digital Teams
- All Staff

5. Fraud and Scam Risk Management Approach

5.1. Prevention Measures

Provide details on prevention measures.

5.2. Detection and Disruption

Provide details on fraud and scam detection and disruption measures.

5.3. Staff Training

Provide details of ongoing training for frontline and fraud teams on scam typologies and escalation protocols.

6. Incident Response and Customer Engagement

6.1. Response Protocols

Outline internal protocols for fraud and scam events including containment actions and engagement with law enforcement, relevant regulators, and broader industry.

6.2. Customer Communication

Outline internal protocols for communicating with customers during an incident.

7. Managing Risk for Persons Experiencing Vulnerabilities Customers

Outline how vulnerabilities will be detected and managed.

8. Metrics, Targets, and Continuous Improvement

8.1. Performance Measurement

Outline metrics to monitor effectiveness for example:

- Number of scam/fraud incidents detected.
- Value of losses prevented vs. losses incurred.
- Response and resolution times.
- Volume and resolution of customer complaints related to fraud.
- Number of staff trained and retrained.

8.2. Targets

Outline targets for fraud and scam prevention for example:

- Year-on-year reduction targets for fraud incidents.
- Targets for staff training completion and customer scam education outreach.
- Increase in early detection and prevention rates.

8.3. Policy Review and Improvement

Outline the process for review and continuous improvement for example:

- Annual review of policy (or more frequently post-incident or regulatory update).
- Benchmarking against industry standards and APRA/ASIC expectations.
- Use of fraud analytics and data trends to evolve prevention and detection measures.
- Use of stakeholder and customer feedback to refine processes.

9. Compliance Monitoring

Outline how compliance with this policy and regulator expectations will be monitored.

10. APPENDIX C: Superannuation Fund Members of the FSC

- AMP
- Australian Ethical
- Betashares
- Brighter Super
- BT Financial
- Care Super
- Challenger
- Colonial First State
- Equity Trustees
- Hub24
- ING
- Insignia Financial (including MLC, OnePath, and IOOF)
- Macquarie
- Mercer
- Netwealth
- Vanguard

FSC Standard No. 29

11. APPENDIX D: Relevant Legislation and Regulation Considered in the Creation of this Standard

Legislation

- Superannuation Industry (Supervision) Act 1993 (SIS Act) (**Link**)
- Superannuation Industry (Supervision) Regulations 1994
- Scams Prevention Framework Act 2025 (**Link**)

APRA Prudential Standards and Guidance

- Prudential Standard SPS 220 – Risk Management (**Link**)
- Prudential Practice Guide SPG 223 – Fraud Risk Management (**Link**)
- Prudential Standard CPS 230 – Operational Risk Management (**Link**)
- APRA Letter to Superannuation Trustees (June 2025) – For Action: Information Security Obligations and Critical Authentication Controls (**Link**)

ASIC Regulatory Guidance and Instruments

- Regulatory Guide RG 271 – Internal Dispute Resolution (**Link**)
- Report 790: Anti-Scam Practices of Banks Outside the Four Major Banks (**Link**)
- ASIC Letter to Superannuation Trustees (Jan 2025) (**Link**)