asfa
the voice of super

Minimum Fraud Controls for Superannuation Funds

Updated: August 2025

ASFA has been operating since 1962 as the peak policy, research and advocacy body for Australia's superannuation industry. ASFA represents the APRA regulated superannuation industry with over 100 organisations as members from corporate, industry, retail and public sector funds, and service providers.

We develop policy positions, service standards and practice guidance through collaboration with our diverse membership base and use our deep technical expertise and research capabilities to assist in advancing superannuation and retirement outcomes for Australians.

The Association of Superannuation Funds of Australia Limited (ASFA)
PO Box 1485, Sydney NSW 2001
T +61 2 9264 9300 or 1800 812 798 (outside Sydney)

ABN 29 002 786 290
ACN 002 786 290

www.superannuation.asn.au

1

Background

Large scale data breaches have highlighted how cybercrime, identity theft and fraud pose increased threats throughout the economy including financial services. Superannuation funds are not immune and continue to see increased activity by fraudulent cyber criminals seeking to gain access to members' data and retirement savings. There is a growing risk to fund members through loss of individuals savings.

Recent events resulting in unauthorised access to member data and, in a small number of cases financial losses for members, demonstrate that superannuation funds remain a viable target for cyber criminals. Raising the minimum level of authentication controls helps to mitigate the most common attack techniques used by cyber criminals, such as "credential stuffing" [1].

Previous guidance on multi-factor authentication permitted funds to make risk-based decisions regarding its application in the online process. However, recent events indicate that, despite the initial friction introduced during login, the drawbacks of not implementing it for all members at the initial login stage significantly outweigh any inconvenience experienced by users. ASFA's updated guidance aligns with regulatory expectations and best practices in the financial services sector, better representing its expectations of member organisations.

Superannuation funds already have obligations to conduct identity checks on members for certain transactions (for example, rollovers between APRA-regulated funds). In addition, Know Your Customer (KYC) obligations contained in Anti-Money Laundering/Counter Terrorism Financing (AML/CTF) legislation apply to certain other transactions, requiring verification of a member's identity. This is a non-prescriptive and risk-based process which funds must apply alongside a range of existing fraud protections built into their systems and processes. An individual fund's approach to deploying such protections may vary depending on the fund's risk appetite, the sector the fund belongs to and the profile of its membership.

With the growing risk of scams and fraud, and the increasing sophistication of these threats, the superannuation industry has a role to play in ensuring the security of members' savings.

[1] Credential stuffing is a common technique where attackers use a list of compromised user credentials (username + password) to access a system. The attack uses bots for automation and scale and is based on the assumption that many users reuse usernames and passwords across multiple services.

ASFA has developed a range of minimum standard controls for funds to apply consistently across certain transactions in the superannuation account lifecycle. The development of these minimum controls builds on current industry practice while improving in some areas.

This will fortify the superannuation industry's shared defences against fraudulent criminals by reducing the risk associated with unauthorised account access and loss of members' retirement savings from the system.

The table below defines key events and vulnerabilities in the superannuation account lifecycle from a fraud perspective, as well as proposed minimum control requirements that funds should implement. It is acknowledged that funds may also implement additional system-wide controls to detect fraud activity.

The key controls relate to the following transactions:

1. Creation of new web-based member-initiated accounts
2. Member account login
3. Change of contact details initiated directly by the member
4. SuperMatch request by a member
5. Consolidation and rollover between APRA regulated funds
6. Consolidation and rollover from APRA regulated funds to SMSF
7. Withdrawal or pension commencement

Commencement – Given that cyber criminals are actively targeting the industry, the updated MFA controls take effect immediately, and funds should prioritise the implementation of MFA at member login as soon as possible. To align with APRA's letter relating to *Information Security Obligations and Critical Authentication Controls*, this should be implemented by 31 August 2025, at the latest.

Account Lifecycle	Scope	Event Description	Risks	Current Verification	Current fund Controls	ASFA Minimum Requirements
1) Creation of new web-based member initiated account	Does not include employer accounts, accounts created through a financial adviser, or paper-based account creation by a member.	A new account is opened in a fund by a member using an online account creation process.	'Staging' account created using fraudulent details to test fund processes, link to myGov, control a legitimate account and effect a rollover to a new fund. Can lead to increase in compromised myGov accounts including to access govt benefits.	No Know Your Customer (KYC) requirement. Trustee assessment is risk based.	Not universal. Controls vary from collection of standard personal details through to requiring electronic ID verification, combined with other fund system wide fraud monitoring and screening techniques.	KYC - electronic ID using the Document Verification Service (DVS) to verify member, or document-based verification.
2) Member account login	Includes all member account logins.	Member logs in to account with username and password.	Unauthorised account access with compromised credentials allows viewing of sensitive information or facilitates fraudulent activity.	User credentials (Username and password).	Not universal. Controls vary from Multi-factor authentication at login to threshold based applied.	Multi-factor authentication applied at initial login **and** for specific threshold events.

Account Lifecycle	Scope	Event Description	Risks	Current Verification	Current fund Controls	ASFA Minimum Requirements
3) Change of contact details initiated directly by a member	All accounts*. Does not include change of account details by an authorised person (financial adviser) acting on member's behalf. Does not include change of account details by an authorised person (financial adviser) acting on member's behalf.	Member information added for first time member info changed – e.g. address, phone number, email.	Increase in compromise of phone numbers, email addresses – e.g. fraudster accesses account and changes details to effect rollover or withdrawal.	No KYC requirement. However, a Proof of Identity check (or account ownership check) is performed. Trustee assessment is risk-based.	Funds generally apply Multi-Factor Authentication (MFA) or similar method (e.g. member portal) to contact the member to verify these changes. However, the application of these techniques is not universal.	Multi-Factor Authentication (MFA), push notification via SMS and/or email, and/or a prompt to access member portal to authorise completion of transaction. Change of mobile phone number should require confirmation via the existing and new phone numbers.
4) SuperMatch request by a member	All accounts	Funds request a list of active information for a member from ATO.	Connect SuperMatch to newly opened fraudulent account. Discovery of existing accounts often followed by rollover of member funds into fraudulent account.	KYC must be completed (electronic or document-based) to a prescribed level* before the fund can activate a SuperMatch search.	As per prescribed SuperMatch requirements.	As per prescribed SuperMatch requirements.

Account Lifecycle	Scope	Event Description	Risks	Current Verification	Current fund Controls	ASFA Minimum Requirements
5) Consolidation and rollover between APRA funds	All accounts	Movement of money (part of full balance) from one fund to another or within a fund.	Unauthorised movement of member balances into fraudulent APRA fund account.	KYC not required. Member must provide the transferring fund with: their name, address, date of birth and Tax File Number (TFN). Fund then checks the details match those on their system and validates the TFN with the ATO. Three-day rule: benefits required to be rolled over within the later of three business days of receiving the rollover request or the fund receiving all mandatory information (including any Suspicious Matter Reports (SMRs) requiring enhanced due diligence).	Varies from SMS/email notifications to risk-based verifications deployed in certain instances if a system control flags a concern.	Push notifications (SMS or email) to make member aware of request to rollover. Ideally a series of alerts at key stages of transaction. (Given the Three-day rule, using MFA to authorise a rollover can currently act as a potential barrier and may not be preferred. Whilst a push notification does not provide complete assurance that the member responds to a fraudulent attempt within the timeframe in all cases, the centralised fraud register would bolster a funds ability to claw back funds where necessary).

Account Lifecycle	Scope	Event Description	Risks	Current Verification	Current fund Controls	ASFA Minimum Requirements
6) Consolidation and rollover from APRA fund to SMSF	All accounts	Movement of money (part of full balance) from an APRA fund to an SMSF.	Rollover to SMSF using fraudulent identity which passes KYC protocols. Fraudulent bank account on SMSF used (unable to be detected).	KYC must be completed. Process is non-prescriptive and risk based. 3-day rule benefits required to be rolled over within the later of 3 business days of receiving the rollover request or the fund receiving all of the mandatory information (after KYC and bank check completed).	KYC must be completed Process is non-prescriptive and risk based. Funds use either electronic ID (using DVS) or document based. Additional controls may also be applied.	Push notifications (SMS or email) to make member aware of request to rollover. Ideally a series of SMS alerts at key stages **or** Member authentication^ (completed on a risk- based approach and/or based on materiality).

Account Lifecycle	Scope	Event Description	Risks	Current Verification	Current fund Controls	ASFA Minimum Requirements
7) Member requests a benefit paid or pension commenced	All accounts	Request to access balance through lump sum withdrawal, commencing a pension or early release.	Unauthorised movement of member balances out of system or to commence pension using fraudulent identity documentation.	KYC must be completed. Process is non-prescriptive and risk-based.	KYC must be completed – process is non-prescriptive and risk-based. Funds use either electronic ID (using DVS) or document based. Additional controls may also be applied.	MFA, push notification via SMS or email, or prompt to access member portal to authorise completion of transaction. **or** Member authentication^ (completed on a risk- based approach and/or based on materiality). [It is not envisaged either of these requirements would be imposed with each regular partial withdrawal.]

*Minimum requirements under SuperMatch: Electronic-based verification - for electronic-based verification the customer's name and either their address or date of birth or both must be verified against two reliable and independent electronic data and must include at least one primary Government ID verified against the Document Verification Service (DVS) where applicable.

Document-based verification: for document-based verification the customer's name and either their address or date of birth, or both, must be verified against: an original or certified copy of a primary photographic identification documentnboth: an original or certified copy of a primary non-photographic identification document an original or certified copy of a secondary identification document. and any document used for verification must not have expired (other than an Australian passport which can be used if it expired within the past 2 years).

Customer verification is not a once off event and must be ongoing to ensure the individuals identity has not been compromised. Where there is no positive activity from the member on their account for a period of two years, the trustee must complete customer verification to the minimum level prescribed above before the SuperMatch service can be used for that member.

^ Authentication: this refers to a member verifying that they are the member linked to that account and being able to provide assurance that they are the member that requested a payment. Currently, where this is completed, there are a range of techniques used from phone call or video call to selfie ID.

Separately, verification in this context refers to the collection of details about a member's identity and checking them against authoritative sources of identity data to confirm a match (e.g. via DVS) or ensuring the documentation proving the identity is certified.

The Association of Superannuation Funds of Australia Limited (ASFA)
PO Box 1485, Sydney NSW 2001
T +61 2 9264 9300 or 1800 812 798 (outside Sydney)

ABN 29 002 786 290
ACN 002 786 290

asfa
the voice of super