ASFA Better Practice Guidance: Minimum fraud controls for superannuation funds

Background

Recent, 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 actors seeking to gain access to members' data and retirement savings. There is a growing risk to fund members through loss of individuals savings.

Superannuation funds have a range of existing obligations relating to identity checks in relation to members for certain transactions (e.g. 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 fraud, and the increasing sophistication of these threats, the superannuation industry has a role to play in ensuring the security of members' savings.

ASFA has developed a range of minimum standard controls (in the table below) for funds to apply consistently across certain transactions in the superannuation account lifecycle. The development of these common minimum controls harnesses current industry practice and makes enhancements in certain areas. This will fortify the superannuation industry's shared defences against fraudulent actors by reducing the number of fraudulent accounts created and preventing the loss of members' retirement savings from the system.

The table below defines key events and relevant vulnerabilities in the superannuation account lifecycle from a fraud perspective, and proposed common minimum control requirements funds should deploy. It is acknowledged funds may also conduct other system-wide controls to detect fraud activity. The key controls relate to the following transactions:

1. the creation of new web-based member-initiated accounts
2. a change of contact details initiated directly by the member
3. rollovers between APRA regulated funds
4. rollover from APRA regulated fund to SMSF and
5. withdrawal or pension commencement.

Commencement - the controls should be in place from no later than 1 July 2024. However, funds should be permitted to stagger their implementation over 12 months to the full introduction of the requirements from this date – with funds assessing and prioritising the key/immediate risks earlier in the transition.

Account Lifecycle	1) Creation of new web-based member-initiated account	2) Change of contact details initiated directly by a member	SuperMatch request by a member	3) Consolidation and rollover between APRA funds	4) Consolidation and rollover from APRA fund to SMSF	5) Member requests a benefit paid or pension commenced
	*Does not include employer accounts, accounts created through a financial adviser, or paper-based account creation by a member	*All accounts. Does not include change of account details by an authorised person (financial adviser) acting on member's behalf	All accounts	All accounts	All accounts	All accounts
Event description	A new account is opened in a fund by a member using an online account creation process.	Member information added for first time member info changed – e.g. address, phone number, email.	Funds request a list of active information for a member from ATO	Movement of money (part of full balance) from one fund to another or within a fund.	Movement of money (part of full balance) from an APRA fund to an SMSF.	Request to access balance through lump sum withdrawal, commencing a pension or early release.
Key risks / vulnerabilities	'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.	Increase in compromise of phone numbers, email addresses – fraudster accesses account and changes details to effect rollover or withdrawal.	Connect SuperMatch to newly opened fraudulent account. Discovery of existing accounts often followed by rollover of member funds into fraudulent account	Unauthorised movement of member balances into fraudulent APRA fund account	Rollover to SMSF using fraudulent identity which passes KYC protocols. Fraudulent bank account on SMSF used (unable to be detected).	Unauthorised movement of member balances out of system or to commence pension using fraudulent identity documentation.
Current verification requirements	No Know Your Customer (KYC) requirement. Trustee assessment is risk based	No KYC requirement. However, a Proof of Identity check (or account ownership	KYC must be completed (electronic or document-based) to	KYC not required. Member must provide the transferring fund with: their name,	KYC must be completed – process is non-prescriptive and risk-based.	KYC must be completed – process is non-prescriptive and risk-based.

Account Lifecycle	1) Creation of new web-based member-initiated account	2) Change of contact details initiated directly by a member	SuperMatch request by a member	3) Consolidation and rollover between APRA funds	4) Consolidation and rollover from APRA fund to SMSF	5) Member requests a benefit paid or pension commenced
		check) is performed. Trustee assessment is risk-based	a prescribed level* before the fund can activate a SuperMatch search.	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).	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).	
Current fund controls	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.	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.	As per prescribed SuperMatch requirements	Varies from SMS/email notifications to risk-based verifications deployed in certain instances if a system control flags a concern	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	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

Account Lifecycle	1) Creation of new web-based member-initiated account	2) Change of contact details initiated directly by a member	SuperMatch request by a member	3) Consolidation and rollover between APRA funds	4) Consolidation and rollover from APRA fund to SMSF	5) Member requests a benefit paid or pension commenced
Minimum requirement – *ASFA Better practice* **(in addition to existing regulatory requirements)**	KYC - electronic ID (using the Document Verification Service (DVS)) to verify member, or document-based verification.	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.	As per prescribed SuperMatch requirements	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).	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).	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 document
- both: 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.