

Industry specific guidance: Superannuation sector

Contents

Purpose	2
Using this guidance	2
AML/CTF obligations.....	3
ML/TF risks in the sector.....	3
Mitigating ML/TF risk in the sector.....	34
AML/CTF programs	34
Risk assessments	34
Customer due diligence	45
Transaction monitoring program.....	45
Suspicious matter reports.....	45
Worked examples.....	5
Fraud: Early release of superannuation using falsified documents.....	56
Money laundering: Possible tax evasion/proceeds of crime	67
Outsourcing AML/CTF obligations	78
Cyber-enabled crime (1): unusual activity.....	89
Terrorism financing: self-funded foreign terrorist fighter.....	940
Illegal early release: multiple hardship claims	1044
Politically exposed persons	1142
Employee due diligence	1243
Cyber-enabled crime (2): identity takeover	1344

Purpose

This guidance is to assist reporting entities in the superannuation sector to better understand their anti-money laundering/counter-terrorism financing (AML/CTF) obligations, with reference to industry-specific risks. It also explains how entities can use their 'AML/CTF toolkit' to lessen and respond to the money laundering/terrorism financing (ML/TF) risks they face.

This guidance was developed in response to:

- the need to provide tailored guidance for superannuation funds about their obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act)
- risks identified in AUSTRAC's [risk assessment of the superannuation sector](#), to provide insights into combating those risks—AUSTRAC assessed the overall ML/TF risk for the sector as 'medium'.

AUSTRAC collaborated with the Australian Institute of Superannuation Trustees and the Financial Services Council of Australia - and their respective members - when developing this guidance.

Using this guidance

The AML/CTF framework supports a risk-based approach, allowing reporting entities to determine the most effective and proportionate ways to identify, mitigate and manage ML/TF risk.

Different superannuation funds have different risk profiles. Factors that may influence risk include:

- characteristics of the fund's membership, including the industry sector(s)
- the range and scope of products on offer
- delivery channels of these products, including the use and application of new technologies
- specific business processes and practices.

Entities should consider how this guidance can be applied in the context of their own risk profiles. The guidance contains hypothetical examples and responses that may be considered 'good practice' in the given scenarios.

This guidance is not intended to be prescriptive or exhaustive. It aims to assist superannuation funds to recognise how they can identify, manage and mitigate risks.

This guidance does not replace the [AUSTRAC Compliance Guide](#). It should be used and read in conjunction with that guide, the AML/CTF Act and AML/CTF Rules.

This guidance will be reviewed and updated when required.

AML/CTF obligations

Trustees of superannuation funds have obligations under the AML/CTF Act when they:

- accept a contribution, rollover or transfer in relation to a member
- pay out an interest held by a member.

Funds are also subject to other regulatory obligations (such as those administered by the Australian Taxation Office and the Australian Prudential Regulation Authority). These can be complementary to the management of ML/TF risk.

The sector can use these obligations as part of their AML/CTF toolkit to identify and respond to ML/TF risks.

ML/TF risks in the sector

AUSTRAC's [risk assessment of the superannuation sector](#) identified scenarios and characteristics that may make the sector vulnerable to ML/TF.

The scenarios used in this guidance reflect these vulnerabilities, and provide possible ways to address and manage the associated risks. This guidance does not cover every risk or product relevant to the superannuation sector.

Mitigating ML/TF risk in the sector

The compliance and reporting obligations in the AML/CTF Act and Rules maintain the integrity of Australia's AML/CTF regime and provide reporting entities with tools to identify, mitigate and manage ML/TF risk. For example, a reporting entity can identify patterns of suspected criminal activity through the use and application of ongoing customer due diligence and transaction monitoring, and submitting suspicious matter reports (SMRs) to AUSTRAC. These obligations are complementary to applying sound compliance practices designed to protect the business and its customers.

AML/CTF programs

Reporting entities are required to establish, implement and maintain an AML/CTF program. This is an integral and fundamental component of Australia's AML/CTF regime. AML/CTF programs outline a reporting entity's policies and approach to identify, mitigate and manage ML/TF risk.

Risk assessments

A reporting entity's risk assessment should be flexible, dynamic, and responsive, to reflect changes in the entity's risk profile. This includes consideration of new and emerging risks.

Reporting entities in the superannuation sector should be familiar with risks relevant to the sector as a whole (including those discussed in AUSTRAC's ML/TF risk assessment and the

'worked examples' in this guidance). They should also consider risks specific to their business—for example, whether the reporting entity provides other designated services.

In addition to considering characteristics of customers that may make them high risk, the reporting entity should also consider whether characteristics of the employer of those customers change the risk profiles. For example, an employer may present higher ML/TF risk if it has been the subject to adverse criminal or civil findings, or if it deals with industries known for their dependency on the use of physical cash.

Customer due diligence

Customer due diligence (CDD) is a cornerstone of the AML/CTF regime and covers every stage of the relationship with the customer. Particular transactions or events may prompt a reporting entity to re-identify a customer, or apply enhanced CDD—for example, where the customer may be a ~~domestic~~ 'politically exposed person' (PEP).

Superannuation funds are not *required* to identify their customers at the commencement of the customer relationship, or upon receipt of contributions or rollovers. However, reporting entities should adopt a flexible approach to dealing with any perceived ML/TF risk, such as by choosing to identify their customer earlier in the customer relationship. For example, if a new superannuation account holder presents a higher level of risk, the reporting entity can apply CDD measures as soon as practicable, to determine the nature and extent of that risk, and use ongoing and enhanced due diligence processes as required.

Commented [PC1]: We have received comment that this should not be confined to domestic persons but also may apply to international PEPs.

Transaction monitoring program

The requirement for a reporting entity to conduct CDD also includes the obligation to monitor transactions. Generally, the Trustees of a superannuation fund retain the legal responsibility for the operation of a ~~transaction monitoring~~ **transaction monitoring** program. This includes circumstances where it has been outsourced to a third party—for example, to the administrator of a superannuation fund.


Trustees of superannuation funds should also consider the nature of transaction monitoring arising from their ML/TF risk profile. They should also consider whether transaction monitoring by an external provider should be supplemented with additional transaction monitoring or business intelligence systems. This decision must be informed by the reporting entity's assessment of its ML/TF risk, and the effectiveness of the outsourced transaction monitoring processes to identify and flag particular higher risk transactions or customers. Outsourced transaction monitoring conducted by an administrator or another provider should also be subject to regular review and testing.

Suspicious matter reports

Submitting SMRs is a critical obligation under the AML/CTF Act. A suspicion may be formed based on incomplete information—a partially completed SMR can help AUSTRAC or one of its partners build a more comprehensive financial intelligence picture.

Worked examples

The worked examples are for illustrative purposes only, to highlight how the AML/CTF toolkit can be used to identify, mitigate and manage industry-specific ML/TF risks. The worked examples provide insights into how the sector can adopt flexible approaches to using their AML/CTF toolkit, in line with their own business and risk profiles. These examples are not prescriptive or exhaustive.

 Each example covers some key themes. Further information on the themes [are](#) in the [AUSTRAC Compliance Guide](#):

[ML/TF risk assessments](#)

[AML/CTF programs](#)

[Customer due diligence](#)

[SMR reporting](#)

[Transaction monitoring](#)

[Employee training](#)

Fraud: Early release of superannuation using falsified documents



Fact: The illegal early release of superannuation can facilitate theft of member funds or the laundering of proceeds of crime.



Scenario: Super Fund A regularly monitors:

- whether the customer's transactions are consistent with the purpose of a superannuation account
- whether the customer's transactions are consistent with the customer's profile
- the nature of its engagement with the customer
- the claims made to support any request for early release, in the context of their accumulated knowledge of particular medical conditions.



Issue: Super Fund A has noticed an increase in requests for the early release of superannuation on the grounds of a debilitating or terminal medical condition. **Super Fund A** requires that these applications include two separate medical certificates, and routinely verifies that each issuing doctor has a current registration.

Super Fund A notices that a cluster of customers from a particular region have obtained medical certificates from two particular doctors. Some of these customers have recently made additional contributions to their policies. Further, **Super Fund A** discovers that a number of these certificates claim the same medical condition and prognosis. The doctors who appear to have provided the certificates practice in locations several hundred kilometers

from where this cluster of customers resides. **Super Fund A** is also concerned that the certificates appear to be fraudulent copies of legitimate certificates.



Response: **Super Fund A** already has in place systems and processes to detect activity that may be suspicious, including fraudulent applications for early release.

☑ **Super Fund A** considers that the documents lodged in support of the claims are fraudulent. While **Super Fund A** has not completed an investigation into all of the circumstances, **Super Fund A** decides that the information it holds *could* be relevant to the investigation of an offence, and reports one or more SMRs to AUSTRAC.

☑ On discovering the activity, **Super Fund A** revisits its ML/TF risk assessment and determines that these customer relationships may pose higher ML/TF risk.

☑ **Super Fund A** raises the matter with its administrator and seeks advice on enhancing the claims assessment process to identify potentially illegal applications for early release.

☑ **Super Fund A** changes its documentation and updates its website to better explain the permitted grounds for early release. **Super Fund A** advises its members that medical certificates may be verified with the treating doctor(s), and requires that the member consent to this happening.



Discussion: **Super Fund A** has mechanisms in place to manage ML/TF risk. These include identifying patterns of activity that may indicate suspicious behaviour, and carrying out CDD (including enhanced CDD when unusual transactions occur).

Money laundering: Possible tax evasion/proceeds of crime




Fact: Voluntary member contributions represent a higher ML risk due to the potential difficulty in establishing the source of funds. In their capacity as payers of super contributions, employers also represent a potential risk for illegal activity.

❓ **Scenario:** **Super Fund C** is the default super fund for **AB Pty Ltd**. **AB Pty Ltd** operates in an industry with high levels of cash turnover. In accordance with its AML/CTF program, **Super Fund C** pays closer attention to members that are employed in high-cash industries. **Super Fund C** has developed a typical member profile and is able to detect, through its transaction monitoring program, members whose behaviour is inconsistent with the typical customer profile.

⚠ **Issue:** **Super Fund C** notices that a number of employees of **AB Pty Ltd** have significantly increased their voluntary super contributions (well above concessional tax thresholds). The contributions do not align with the customer profiles, and there are no known corresponding increases in salaries. **Super Fund C** has also identified a large increase in membership applications from employees of **AB Pty Ltd** that contain inconsistencies. Several applications included the same, or similar, name and date of birth details.

Super Fund C suspects that employees of **AB Pty Ltd** may be receiving undeclared income in cash. This would allow the employees to use the undeclared cash income for living

expenses, while diverting more of their declared regular earnings into superannuation. **Super Fund C** also suspects that **AB Pty Ltd** may be registering fake employees.

 **Response:** **Super Fund C** already has in place systems and processes to detect activity that may be suspicious, including large contributions that are inconsistent with the member's profile, and anomalies in new policy applications. **Super Fund C** has also already ceased accepting cash contributions from its members, due to the high-risk nature of cash, and the difficulty in establishing source of funds.


☑ Despite not providing a designated service to **AB Pty Ltd**, **Super Fund C** is concerned by the seemingly fraudulent policy applications, and decides to conduct due diligence on **AB Pty Ltd** and its beneficial owners. It finds that a manager of **AB Pty Ltd** is currently disqualified from 'involvement in the management of a corporation'.

☑ **Super Fund C** decides to more fully identify employees of **AB Pty Ltd** whose contributions are inconsistent with the customer profile, and whose policy applications appear anomalous.


☑ **Super Fund C** writes to a number of employees of **AB Pty Ltd** to request certified copies of identification documents.


☑ **Super Fund C** forms a suspicion about the members whose contributions do not align with their customer profiles, as they are unable to determine whether the source of funds is from legitimate means. **Super Fund C** submits SMRs on these members, as well as those who did not provide the requested identification documents. **Super Fund C** also notes the employment relationship between the employee and **AB Pty Ltd**.


☑ **Super Fund C** fine-tunes its transaction monitoring rules to flag unusual changes to member contributions and anomalies in policy creation applications.

 **Discussion:** In this scenario, **AB Pty Ltd** may be paying its employees with cash proceeds of criminal activity. The employees may be accepting undeclared income and diverting legitimate income into their super policies.

Outsourcing AML/CTF obligations

 **Fact:** Reporting entities retain legal responsibility for AML/CTF Act compliance, even when functions are outsourced.

 **Scenario:** **Super Fund D** has a contract with **I-dee Ltd**, for **I-dee Ltd** to conduct customer identification on **Super Fund D**'s members, and monitor members' transactions. The contract prescribes the measures to be undertaken by **I-dee Ltd**, and allows **Super Fund D** to monitor and regularly test **I-dee Ltd**'s systems and processes.

 **Issue:** **Super Fund D** recently received phone calls from a number of members with post-preservation policies, claiming they have not received their last regular super income stream payment. **Super Fund D** identifies that for affected members' policies:

- recent requests have been received to change the members' details, including their nominated bank account for super income payments
- proof of identity to support the requested changes was verified electronically

- subsequent requests were received to significantly change the members' payment amounts and frequency
- the transactions appear inconsistent with the expected customer profiles, and all previous transaction history for those customers
- the requests to change the payment amount and frequency were processed shortly after a new function was introduced that allowed members to make changes to their income stream payments via an online portal.



Response:

☑ **Super Fund D** is concerned that the members' policies may have been compromised as a result of sophisticated identity theft and takeover. **Super Fund D** submits SMRs to AUSTRAC.

☑ **Super Fund D** immediately contacts other members with a similar transaction history to verify the requested changes to their policies.

☑ **Super Fund D** works with **I-dee Ltd** to fine-tune transaction monitoring processes, to flag activity such as changing income stream payment details and/or requesting lump-sum payments directly after customer's details have been changed.

☑ **Super Fund D** introduces a new process for contact centre staff to phone the members who have made online changes to their payment preferences, to verify those changes.



Discussion: **Super Fund D** knows that as a reporting entity, it retains legal responsibility for compliance with the AML/CTF Act. **Super Fund D** needs to be satisfied that **I-dee Ltd** is adequately carrying out the functions for which it has been contracted.

Cyber-enabled crime (1): unusual activity



Fact: Criminals are known to target superannuation to steal member funds. Risks can arise when members can access and update their personal information online.

❓ **Scenario:** **Super Fund E** allows its members to access information about their superannuation policies online. Members can update their profile and personal information using a dedicated online portal and secure log-in process. **Super Fund E** has implemented systems to detect and collect information about the device accessing a member policy, in a manner compliant with privacy legislation. To further mitigate the risk of fraudulent activity, **Super Fund E** conducts regular testing of these systems. **Super Fund E** also promotes member awareness of cyber security issues.

⚠ **Issue:** **Super Fund E** notices that the policy of its member, **John Citizen**, has been accessed via multiple electronic devices. On a number of occasions, the security question for the policy was not answered correctly. **Super Fund E** investigates the pattern of logins and suspects that more than one person has been accessing **Mr Citizen's** policy.

Super Fund E then receives a request for withdrawal via **Mr Citizen's** email address.



Response:

- ☑ **Super Fund E** establishes that the electronic device used to submit the withdrawal request has previously been used to successfully answer the security questions on the policy.
- ☑ **Super Fund E** contacts **Mr Citizen** by telephone to confirm the details of the withdrawal.
- ☑ After **Mr Citizen** confirms the withdrawal request is legitimate, **Super Fund E** advises **Mr Citizen** that his policy has been accessed through a number of different devices, seemingly by multiple individuals. **Super Fund E** suggests that **Mr Citizen** change his password and provides a copy of the 'Protecting your super account from fraud' fact sheet.
- ☑ **Super Fund E** decides to investigate implementing two-factor verification technology.
- ☑ After **Mr Citizen** changes his password, **Super Fund E** receives another request via email to withdraw the balance of the policy. On this occasion, when carrying out customer due diligence, **Super Fund E** is not satisfied that **Mr Citizen** has identified himself. Even though **Mr Citizen** does not appear to be complicit, **Super Fund E** is concerned about possible attempted fraud and submits an SMR detailing the activity on **Mr Citizen's** policy.
- ☑ **Super Fund E** uses its transaction monitoring systems to place an alert on **Mr Citizen's** policy to detect any future unusual activity.



Discussion: **Super Fund E** understands that the use of electronic communication between funds and members creates a favourable environment for cybercrime.

Super Fund E also recognises the potential risks that accompany lack of face-to-face delivery of services, and has implemented processes to mitigate and detect these risks.

Terrorism financing: self-funded foreign terrorist fighter



Fact: Terrorism financing has been identified as a small but emerging and serious threat for the superannuation sector. Where a reporting entity forms a suspicion that relates to terrorism financing, an SMR must be reported to AUSTRAC within 24 hours. Customers of reporting entities may be recorded on 'watch lists' (such as the 'Consolidated List' maintained by the Department of Foreign Affairs and Trade), and engage in behaviour that suggests they intend to undertake illegal activities. Self-managed super funds (SMSFs) can be used to transfer superannuation balances out of the Australian Prudential Regulation Authority (APRA) -regulated sector. Funds can then be withdrawn to bank accounts unrelated to either the member or the SMSF.

❓ **Scenario:** **Super Fund F** has a ~~transaction monitoring~~**transaction monitoring** program that among other things, detects matches for its customers against certain watch lists, sanctions lists, and media reports.

⚠️ **Issue:** **Super Fund F's** transaction monitoring program returned a positive match against an individual on a watch list. Further CDD enquiries, including online research of open source information, located recent Australian media reports suggesting a connection with suspected foreign terrorist fighters. **Super Fund F** reviews the member's policy and finds the following:

- The individual attempted to access their super by claiming financial hardship. This application was denied.

- The individual then requested information about rolling over their balance into an SMSF. The individual noted they had not yet set up an SMSF.
- The individual stated they did not know much about SMSFs, but it did not matter because they were travelling overseas soon.



Response:

☑ **Super Fund F** was not able to confirm the details or existence of an SMSF with the Australian Taxation Office, as the individual had not yet established an SMSF.

☑ **Super Fund F** undertakes a review of the customer's activity, and determines that because the individual has been mentioned in media reports, the activity is suspicious.

Super Fund F submits an SMR to AUSTRAC within the required 24-hour time frame, detailing the engagement with the member.

☑ **Super Fund F's** review highlights a need for further employee training. **Super Fund F** engages an external company to review and update its AML/CTF risk awareness training program, to ensure that employees are aware of the sources of ML/TF risk to their business.

☑ **Super Fund F** also reviews its transaction monitoring program and incorporates additional clauses to detect suspicious activity, such as submitting multiple withdrawal requests after unusual/large deposits.



Discussion: This example highlights the importance of effective transaction monitoring and AML/CTF risk awareness training for employees, as a tool to mitigate ML/TF risk.

Illegal early release: multiple hardship claims



Fact: Superannuation benefits generally cannot be accessed until a member meets the preservation age, as defined by relevant legislation. However, there are some other scenarios in which members can access benefits if a condition for release is met. For example, the Department of Human Services (DHS) allows early release of benefits on the grounds of severe financial hardship, subject to an annual maximum of \$10,000. Once the member satisfies the DHS eligibility criteria, the Trustee is able to release funds to a nominated personal bank account or by cheque.

❓ **Scenario:** **Super Fund G** received an application for membership from customer **Mr Orange**, who then had approximately \$29,000 rolled into his new policy. Two weeks later, **Mr Orange** requested access to those funds on the basis of financial hardship, and presented a letter from DHS supporting his claim. **Super Fund G** paid out the maximum allowed \$10,000. Shortly after, **Mr Orange** requested that the remaining balance of approximately \$19,000 be transferred in equal amounts to two separate funds.


⚠ **Issue:** **Super Fund G** suspects that **Mr Orange** may be abusing the severe financial hardship grounds of release provisions. **Super Fund G** does not know whether **Mr Orange** has also requested release on hardship grounds from the fund that he transferred funds from. The request to transfer amounts under the \$10,000 maximum to separate funds suggests that **Mr Orange** intends to request further releases from those funds.




Response:

☑ **Super Fund G** was not able to satisfy itself that **Mr Orange** only used the financial hardship mechanism once in the given period. **Super Fund G**'s administrator was unable to advise whether **Mr Orange** was known to them through his membership of other funds. **Super Fund G**'s administrator advised that 'anecdotally' this behaviour suggested improper conduct. Super Fund G is aware that some funds require their members to provide consent for the fund to contact the fund from which the member rolled-in their balance.


☑ **Super Fund G** reported an SMR to AUSTRAC.

 **Discussion:** While individual funds may not have an overview of the customer's engagement with the sector as a whole, the reporting of suspicious behaviour to AUSTRAC by regulated businesses can help AUSTRAC identify a customer's dealings with multiple businesses in the financial sector.


Politically exposed persons

 **Fact:** Reporting entities may have customers who are PEPs (domestic or international). PEPs are individuals who occupy a prominent public position or function in a government body or international organisation. Immediate family members and close associates of PEPs are also considered to be PEPs.

Domestic PEPs

 **Scenario:** Under its AML/CTF program, **Super Fund H** assesses if any of its members is a PEP, and considers the risk of dealing with each identified PEP on a case-by-case basis. **Super Fund H**'s transaction monitoring seeks to identify customers who may exercise influence in return for financial benefit.

Jane Person, a member of the fund, is a senior official in a large State Government agency with responsibility for planning and development decisions. **Super Fund H** considers **Ms Person** to be a PEP. **Ms Person** previously worked in the property development industry.

 **Issue:** **Ms Person** receives superannuation contributions from her employer. However, her policy recently started receiving additional fortnightly contributions from a source that is not her employer. **Super Fund H** considers that receiving two sets of regular contributions is inconsistent with the normal member profile. **Super Fund H:**

- is not aware of **Ms Person** having any other sources of income other than her salary package in her senior official role
- is concerned that **Ms Person** may be exposed to corruptive influences in her role
- has not been able to rule out the possibility of a potential conflict of interest.

In this context **Super Fund H** has decided that **Ms Person** poses a medium-high risk.

 **Response:**

☑ **Super Fund H** sought to assess whether **Ms Person** had additional sources of income, and compared her known income and contributions with normal member profile and industry standards.

☑ **Super Fund H** concluded that **Ms Person**'s total contributions, and the fact that she appeared to be receiving contributions from two separate sources, was inconsistent with

normal patterns. This validated its belief that **Ms Person** may be performing her official duties in an inappropriate manner. Alternatively, **Ms Person** may have undeclared income.

☑ **Super Fund H** reported an SMR to AUSTRAC.

☑ **Super Fund H** continued to monitor **Ms Person**'s voluntary contributions.



Discussion: **Super Fund H** has reported an SMR and continues to monitor its relationship with **Ms Person**.

Employee due diligence



Fact: Reporting entities are required to incorporate an employee due diligence program into their AML/CTF program. The employee due diligence program needs to manage the risks posed by personnel who may be able to facilitate the commission of an ML/TF offence in connection with the reporting entity's provision of a designated service.

Businesses that outsource functions are required to ensure that their service providers implement effective AML/CTF controls, including performing employee due diligence. These controls may include:

- probity checks (that is, a National Police Certificate) of relevant employees
- independent written referee checks having regard to the person's honesty and integrity
- an entity-wide code of conduct
- implementation of measures such as recording and/or restricting access to member data and reporting entity systems.

The employee due diligence program must address situations where employees fail to comply with the reporting entity's AML/CTF program.



Scenario: Employee **Mr Smith** recently commenced employment at **Super Fund I**. During the recruitment process, **Mr Smith** did not disclose any convictions.



Issue: A colleague of **Mr Smith** recalls from their industry experience that **Mr Smith** was the subject of a complaint to police by a previous employer, but does not know what the outcome of that complaint was. The colleague brought this to the attention of **Super Fund I**'s Human Resources team, which conducted further research using publicly available information - noting that **Mr Smith** did not disclose this information as required in **Super Fund I**'s employment questionnaire, about whether he was ever investigated, charged or found guilty of a criminal offence. Information of an adverse nature was discovered. Employee **Mr Smith** was invited to respond to the findings of the research, regarding the lack of disclosure.

The Human Resources team investigated the introduction of pre-employment criminal record checks for all new and existing employees in high-risk areas. Accordingly, the Human Resources team invited **Mr Smith** to complete a National Police Certificate application form. When **Mr Smith** was asked again whether he wished to reconsider how he answered the question regarding criminal offences, he admitted that he was found guilty of fraud two years ago, and that he had deliberately not declared the conviction in his employment pack.

After this incident, **Super Fund I** resolved to mandate National Criminal Checks for all existing and new employees.



Response:

Super Fund I now routinely conducts National Police Certificate checks on new employees.

Former employee **Mr Smith**'s conviction and his conduct was found to be incompatible with continued employment at **Super Fund I**. His employment at **Super Fund I** was discontinued.



Discussion: **Super Fund I** identified and responded to a weakness in its employee due diligence processes.

Cyber-enabled crime (2): identity takeover



Fact: Criminals may take over the identities of superannuation fund members in order to steal funds. This can occur through the theft of physical documentation, or via cyber means, such as the interception of electronic communications, or malware infection of electronic equipment. After establishing an account in the name of a real member, criminals may seek to transfer their balances into accounts held in the member's name, but retain control over the operation of the account.



Scenario: **Super Fund J** is a small superannuation fund that has experienced rapid recent growth in its membership. **Super Fund J** notices that across its membership, a surprising number of its non-preserved members have recently arranged for balances from other funds to be rolled into their accounts, and then the balances withdrawn.



Issue: One roll-in transfer was from a member who held an account at **Super Fund K**. Following the processing of this rollover through the SuperStream portal, **Super Fund K** was contacted by the member, who advised that they did not request this rollover. **Super Fund K** immediately contacted **Super Fund J**.

With the consent of the customer, **Super Fund J** and **Super Fund K** conducted an investigation and found that the account at **Super Fund J** had been set up with the correct identifying details about the customer, but with different contact details. The customer provided written confirmation that they had never used the contact details provided to **Super Fund J**.

It was confirmed that the customer's identity had been compromised, and the account at **Super Fund J** had been established by someone other than the customer - a criminal had identified that the member had a balance at **Super Fund K**, through publicly accessible means, and then lodged the request for roll-over, claiming to be the customer.



Response:

Super Fund J and **Super Fund K** concluded that the customer's identity had somehow been compromised and duplicated.

Without informing **Super Fund K** (so as not to breach the tipping-off provisions of the AML/CTF Act), **Super Fund J** reported an SMR to AUSTRAC about the contact details provided by the person who established the customer account.

☑ Without informing **Super Fund J**, **Super Fund K** reported an SMR to AUSTRAC about the fact that its customer's identity had been compromised.

☑ **Super Fund K** advised the member that criminals may seek to exploit the theft of a victim's identity across multiple financial institutions. Accordingly, **Super Fund K** recommended that the member report the incident to police and the Australian Cybercrime Online Reporting Network (ACORN).

☑ **Super Fund K** advised the member to make contact with their other financial service providers to advise them of the identity takeover, and to request a copy of their credit reference information.

☑ **Super Fund J** decided to flag any communications that referred to the email address and telephone number provided, for enhanced CDD.

☑ **Super Fund K** decided that it would confirm all customer roll-out instructions by telephone.



Discussion: **Super Fund J** and **Super Fund K** recognise the increased risks of customer identity theft and fraud that arise with electronic transactions. Both Super funds are aware that they cannot disclose the fact that they have formed a reportable suspicion, except as permitted by the AML/CTF Act.