Australian Government

AUSTRAC

INDUSTRY SPECIFIC GUIDANCE

SUPERANNUATION SECTOR

CONTENTS

PURPOSE

THIS GUIDANCE PROVIDES INFORMATION FOR SUPERANNUATION FUNDS TO ASSIST THEM TO MEET THEIR OBLIGATIONS UNDER AUSTRALIA'S ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING REGIME.

This guidance is to assist reporting entities in the superannuation sector to:

- better understand their obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act)
- identify risks and potential criminal actions arising from the conduct of superannuation funds and their clients,
- explain how these reporting entities can use their AML/CTF 'toolkit' to mitigate the industry-specific money laundering and terrorism financing (ML/TF) risks they face.

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

This guidance is not:

- prescriptive or exhaustive, but aims to assist superannuation funds to identify, manage and mitigate ML/TF risks
- a replacement for the AUSTRAC compliance guide, and should be used and read in conjunction with that guide, as well as the AML/CTF Act and AML/CTF Rules.

The guidance draws on the ML/TF risks identified in AUSTRAC's risk assessment of the superannuation sector. That assessment identified higher than anticipated risks of fraud, cybercrime and terrorism financing in the superannuation sector, and assessed the overall risk of ML/TF activity within the sector as 'medium'.

The risk assessment findings provide the superannuation sector with insights into how they can evaluate and improve their systems and controls to mitigate ML/TF risks.

As the AML/CTF Act supports a risk-based approach to complying with obligations, reporting entities in the superannuation sector should consider how they can apply this guidance in the context of their own risk profiles.

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 offered
- delivery channels of these products, including the use and application of new technologies
- specific business processes and practices.

The guidance contains scenarios where there may be ML/TF risks, and outlines possible ways that may be considered 'good practice' in these circumstances to address and manage the risks. The scenarios illustrate vulnerabilities identified in the superannuation sector risk assessment, but do not cover every risk or product relevant to the superannuation sector.

This guidance will be reviewed and updated when required.

Feedback on the guidance is welcome and can be provided to AUSTRAC via email: contact@austrac.gov.au.

WHEN ARE SUPERANNUATION FUNDS REGULATED UNDER THE AML/CTF ACT?

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 (APRA). 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.

WHAT IS AN AML/CTF TOOLKIT?

The compliance and reporting obligations in the AML/CTF Act and Rules provide reporting entities with tools to identify, mitigate and manage ML/TF risk.

The key obligations in the AML/CTF toolkit are:

- customer due diligence (CDD)
- ongoing customer due diligence (OCDD)
- AML/CTF programs
- record keeping
- reporting.

The obligation for reporting entities to establish, implement and maintain an AML/CTF program is a foundation of Australia's AML/CTF regime. The AML/CTF program outlines a reporting entity's policies, systems and controls for identifying, mitigating and managing ML/TF risk, and sets out the procedures for complying with CDD and OCDD requirements.

Meeting these obligations builds resilience, protecting a reporting entity against misuse for criminal purposes, and provides for the reporting to AUSTRAC of valuable information about financial transactions. AUSTRAC transforms these reports into actionable financial intelligence that can be used by law enforcement, national security and intelligence agencies to combat ML/TF and other serious crime.

Understanding risk

A reporting entity must understand its ML/TF risks and its customers,[1] be able to detect unusual or suspicious customer activity, and manage the risks associated with customer activity that is unusual or suspicious.

A reporting entity's process for assessing and understanding risk should be 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 (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 consider whether characteristics of the employer-sponsor of those customers change the risk profiles. For example, an employer-sponsor may present higher ML/TF risk if it has been subject to adverse criminal or civil findings, or if it deals with industries known for their dependency on the use of physical cash.

Understanding customers

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 '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 considered approach to dealing with any perceived ML/TF risk, such as 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.

Detecting unusual or suspicious transactions

The requirement for a reporting entity to conduct CDD also includes the obligation to undertake ongoing due diligence and monitor transactions. This allows a reporting entity to detect and report unusual or suspicious transactions.

Generally, the trustees of a superannuation fund retain the legal responsibility for the operation of a transaction monitoring program. This includes circumstances where that function 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 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 be subject to regular review and testing.

The ability of reporting entities to detect suspicious customer activity and submit high-quality suspicious matter reports (SMRs) to AUSTRAC is an important pillar of the regime under the AML/CTF Act. A suspicion can be formed based on incomplete information – it is not necessary to fully investigate the customer activity in order to form a suspicion. Information in such an SMR can help AUSTRAC or one of its partners build a more comprehensive financial intelligence picture and detect, prevent and disrupt criminal activity.

[1] In this guidance, the term customer can refer to a fund member

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 is in the AUSTRAC compliance guide:

- ML/TF risk assessements
- 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 for example in this case, 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 terminal medical condition. The superannuation law requires that these applications include two separate medical certificates. **Super Fund A** 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 kilometres 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/contributions. In their capacity as payers of superannuation contributions, employer-sponsors also represent a potential risk for illegal activity.

SCENARIO

Super Fund C is the default superannuation 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 superannuation 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 account 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 account applications. **Super Fund C** 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 account 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 to AUSTRAC 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 account 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 superannuation 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, claiming they have not received their last regular superannuation income stream payment on the scheduled/expected date. **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 superannuation income stream 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 login process. **Super Fund E** has implemented systems to detect and collect information about the device accessing a member account, 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 cybersecurity issues.

ISSUE

Super Fund E notices that the account of its member, **John Citizen**, has been accessed via multiple electronic devices. On a number of occasions, the security question for the account 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** account.

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 for the account.
- **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 account 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 account. 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 to AUSTRAC detailing the activity on **Mr Citizen's** account.
- **Super Fund E** uses its transaction monitoring systems to place an alert on **Mr Citizen's** account 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 superannuation funds (SMSFs) can be used to transfer superannuation balances out of the APRA-regulated sector. Funds are rolled over into an SMSF bank account and can then be withdrawn to other bank accounts unrelated to either the member or the SMSF.

SCENARIO

Super Fund F has a 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 account and finds that the individual:

- attempted to access their superannuation by claiming financial hardship–this application was denied
- then requested information about rolling over their balance into an SMSF, noting they had not yet set up an SMSF
- stated they did not know much about SMSFs, but it did not matter because they were travelling overseas soon.

RESPONSE

- **Super Fund F** is 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 retires, having attained their preservation age, as defined by relevant legislation. However, there are some other scenarios in which members can access benefits if another condition for release is met. For example, the Superannuation Industry (Supervision) Regulations 1994 (SIS Regulations)[2] allow early release of benefits on the grounds of severe financial hardship, subject to an annual maximum of $10,000. Once the member satisfies the relevant SIS Regulations 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 account. Two weeks later, **Mr Orange** requested access to those funds on the basis of financial hardship, and presented a letter from Centrelink that confirmed that **Mr Orange** was in receipt of income support payments. **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** is not able to satisfy itself that **Mr Orange** only used the financial hardship mechanism once in the given period. **Super Fund G**'s administrator is unable to advise whether **Mr Orange** was known to them through his membership of other funds. **Super Fund G**'s administrator advises 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** reports 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.

[2] https://www.legislation.gov.au/Series/F1996B00580

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.

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-sponsor. However, her account recently started receiving additional fortnightly contributions from a source that is not her employer-sponsor. **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 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** seeks to assess whether **Ms Person** has additional sources of income, and compares her known income and contributions with normal member profile and industry standards.
- **Super Fund H** concludes that **Ms Person's** total contributions, and the fact that she appears to be receiving contributions from two separate sources, is inconsistent with normal patterns. This validates 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** reports an SMR to AUSTRAC.
- **Super Fund H** continues 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-sponsor, but does not know what the outcome of that complaint was. The colleague brings this to the attention of **Super Fund I**'s Human Resources team, which conducts 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 is discovered. Employee **Mr Smith** is invited to respond to the findings of the research, regarding the lack of disclosure.

The Human Resources team investigates the introduction of pre-employment criminal record checks for all new and existing employees in high-risk areas. Accordingly, the Human Resources team invites **Mr Smith** to complete a National Police Certificate application form. When **Mr Smith** is asked again whether he wishes to reconsider how he answered the question regarding criminal offences, he admits 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** resolves 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 is found to be incompatible with continued employment at **Super Fund I**. His employment at **Super Fund I** is 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 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 a member's balances into an account held in the member's name, but controlled by the criminal.

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 is from a member who held an account at **Super Fund K**. Following the processing of this rollover through the SuperStream portal, **Super Fund K** is contacted by the member, who advises they did not request this rollover. **Super Fund K** immediately contacts **Super Fund J**.

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

It is confirmed that the customer's identity was compromised, and the account at **Super Fund J** was 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** conclude 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** reports 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** reports an SMR to AUSTRAC about the fact that its customer's identity was compromised.
- **Super Fund K** advises the member that criminals may seek to exploit the theft of a victim's identity across multiple financial institutions. Accordingly, **Super Fund K** recommends that the member report the incident to police and the Australian Cybercrime Online Reporting Network (ACORN).
- **Super Fund K** advises 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** decides to flag any communications that refer to the email address and telephone number provided, for enhanced CDD.
- **Super Fund K** decides that it will 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 funds are aware that they cannot disclose the fact that they have formed a reportable suspicion, except as permitted by the AML/CTF Act.

Australian Government

AUSTRAC