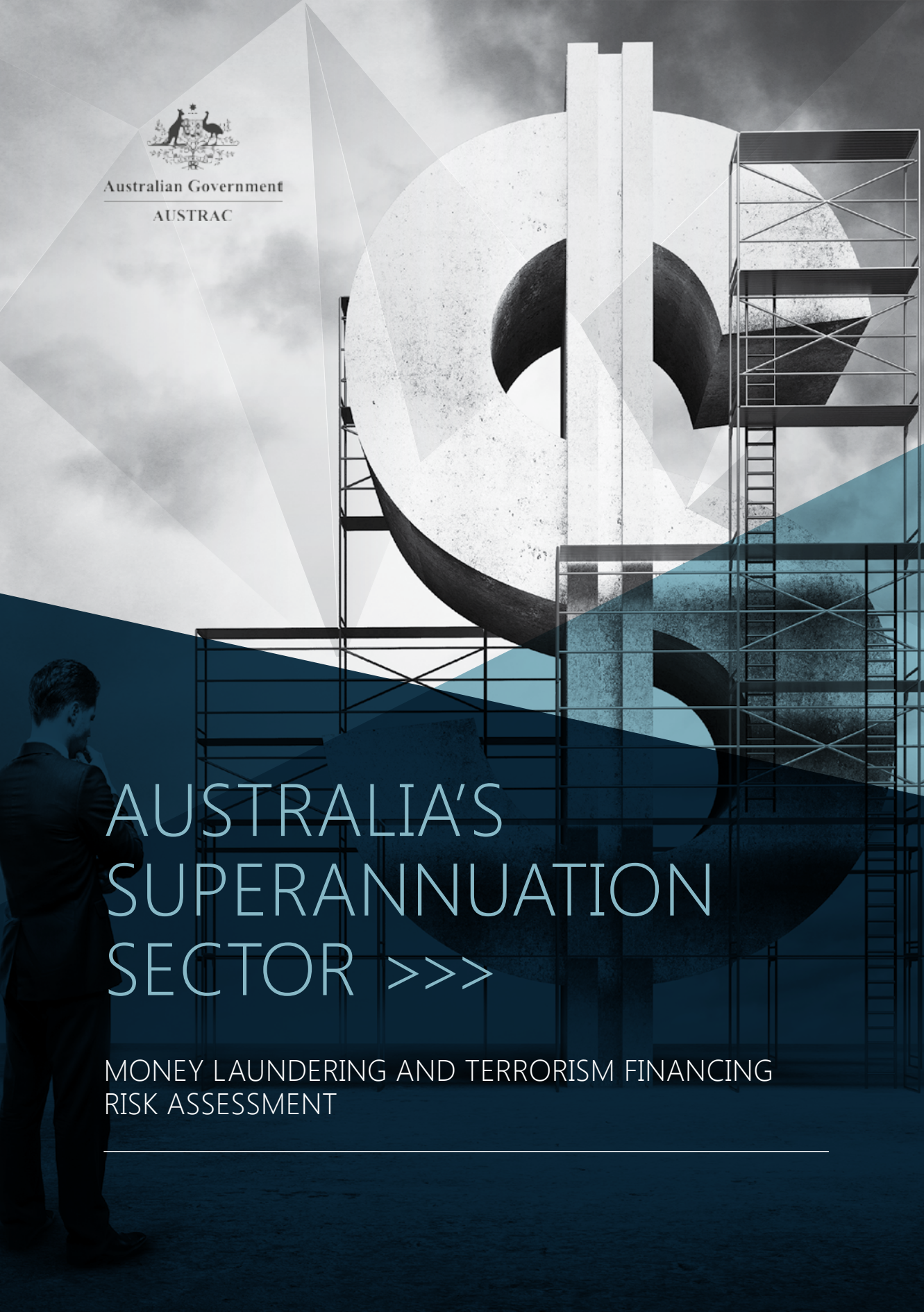


AUSTRALIA'S SUPERANNUATION SECTOR >>>

MONEY LAUNDERING AND TERRORISM FINANCING RISK ASSESSMENT

AUSTRALIA'S SUPERANNUATION SECTOR*

APRA REGULATED SUPERANNUATION FUNDS

242 FUNDS

$1.26 TRILLION IN ASSETS

28M MEMBER ACCOUNTS

$62.8 billion BENEFIT PAYMENTS

$103.9 billion CONTRIBUTIONS

294 SUSPICIOUS MATTER REPORTS SUBMITTED

SUSPICIOUS MATTER REPORTS RELATED TO **PREDICATE OFFENCES**

5 FUNDS REPORTED MORE THAN HALF THE SUSPICIOUS MATTER REPORTS

5 FUNDS REPORTED AT LEAST ONE THRESHOLD TRANSACTION REPORT

SUSPICIOUS MATTER REPORTS RELATED TO **OUTGOING TRANSACTIONS**

*Entities with more than four members. Source: Australian Prudential Regulation Authority, *Quarterly Superannuation Performance Statistics December 2015*, and *Annual Superannuation Statistics Bulletin June 2015* for number of member accounts.

CONTENTS

EXECUTIVE SUMMARY

OVERALL RISK RATING

AUSTRAC assesses the overall money laundering and terrorism financing (ML/TF) risk for the superannuation sector as MEDIUM. This rating is based on an assessment of the criminal threat environment, the vulnerabilities within the sector, and the consequences or harms associated with the criminal threat. This assessment relates to superannuation funds regulated by the Australian Prudential Regulation Authority (APRA).

CRIMINAL THREAT ENVIRONMENT

The criminal threat environment is varied and multifaceted, ranging from opportunistic offences conducted by individual members, to complex and sophisticated attacks executed by organised crime groups, including from entities based overseas.

The size of the superannuation sector ($1.26 trillion in assets)[1] makes it an attractive target for money laundering and associated predicate crimes. Fraud is by far the most prevalent predicate crime, with many reported cases of falsified documents and attempted illegal early release of superannuation savings. Many cases of fraud are enabled by cybercrime, with funds observing regular and sophisticated hacking attempts.

Terrorism financing is a limited but emerging threat. Foreign terrorist fighters (FTFs), who are generally self funded, have accessed superannuation accounts to finance their activities.

VULNERABILITIES

The specific characteristics of the superannuation sector that make it vulnerable to ML/TF and predicate crimes include:

- the extremely large number of member accounts and volume of transactions
- low levels of member engagement, which hampers timely detection of fraud
- post-preservation accounts which have few restrictions on making transactions to and from the accounts
- voluntary contributions to accumulation accounts by members, where the source of money is difficult to verify
- payments to members and outgoing rollovers that are vulnerable to fraud and illegal early release
- the growing reliance on online delivery of products and services, resulting in less face-to-face interaction with customers and increasing online data storage.

1 Australian Prudential Regulation Authority, *Quarterly Superannuation Performance Statistics December 2015.*

In addition, it is highly likely there is significant under-reporting and non-reporting of suspicious matters across the superannuation industry. Just five funds reported more than half of all suspicious matter reports (SMRs) over a two-year period. There is considerable scope for superannuation funds to expand their suspicious matter reporting and strengthen internal controls against financial crime.

Factors that limit the overall vulnerability of the sector include: the relatively simple customer type (mostly individual members); the relatively low level of customer anonymity; the very limited use of cash; and the non-transferability of superannuation accounts between people. The lack of foreign politically exposed persons (PEPs) and the low number of overseas customers and transactions indicate a low foreign jurisdiction risk for the sector.

CONSEQUENCES

The most significant consequences of ML/TF and predicate crimes are generally borne at the individual fund level, particularly for funds with poor internal controls or a weak compliance culture.

Terrorism financing, though to date only involving a few cases, may have significant consequences, including financing the activities of individuals seeking to engage in foreign conflicts and potentially enabling terrorist acts in Australia and overseas.

PURPOSE

This risk assessment provides sector-specific information to the superannuation industry on ML/TF risks. It also covers the main predicate crimes for ML/TF impacting the sector, including cybercrime, fraud and tax evasion.

The information in this risk assessment relates to funds regulated by APRA. These include corporate funds, industry funds, public sector funds and retail funds. It does not specifically assess the risks posed by self-managed superannuation funds (SMSFs), although there is some reference to SMSFs in the assessment.

This risk assessment represents AUSTRAC feedback to the superannuation sector and supports the important collaborative process between government and industry to combat ML/TF in Australia. AUSTRAC expects that this document will assist reporting entities to evaluate and improve the systems and controls necessary to mitigate these risks. Future AUSTRAC compliance activities of this sector will include assessing how reporting entities in the sector have responded to the information in the risk assessment.

Reporting entities should apply information in this assessment in a way that is consistent with the nature, size and complexity of their businesses, and the ML/TF risk posed by their designated services and customers.

METHODOLOGY

The methodology used for this risk assessment follows Financial Action Task Force (FATF) guidance that states when assessing ML/TF risk at the national level, that risk be seen as a function of threat, vulnerability and consequence. In this methodology:

- **Criminal threat environment** refers to the extent and nature of ML/TF and the relevant predicate crimes in a sector.
- **Vulnerability** refers to the characteristics of a sector that make it attractive for ML/TF purposes. This includes features of a particular sector that can be exploited, such as customer types, products and services, delivery channels and the foreign jurisdictions with which it deals. It also considers the level of AML/CTF systems and controls in place across the sector.
- **Consequence** refers to the impact or harm that ML/TF activity may cause.

Twenty-six risk factors are considered across these three categories. An average risk rating is determined for each category, then these ratings determine an overall risk rating for the sector. Further information on the methodology is at Appendix A.

There are three main intelligence inputs that form the assessments and risk ratings:

- Analysis of SMRs and threshold transaction reports (TTRs), as well as other AUSTRAC information and intelligence.
- Reports and intelligence from a variety of partner agencies, including intelligence, revenue, law enforcement, regulatory, anti-corruption and national security agencies across the Commonwealth and state governments.
- Feedback and professional insights offered during interviews and consultations with a range of superannuation fund trustees, fund administrators, industry experts and industry associations.

This risk assessment has benefited from very significant industry collaboration, with some of the most frequent SMR reporters in the sector contributing highly valuable information. These funds – although representing only a small number of entities in the sector – demonstrated a high level of understanding of the ML/TF risk environment, and some described sophisticated strategies used to mitigate these risks. These have been highlighted in this assessment for the benefit of funds across the sector.

SMRs LODGED BY THE SUPERANNUATION SECTOR

Trustees of superannuation funds have reporting obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) when they accept a contribution, rollover or transfer in relation to a member, or cash an interest held by a member. The submission of SMRs to AUSTRAC is a critical obligation under the Act.

AUSTRAC analysed two years of SMRs submitted by the sector through to the end of February 2016.

AUSTRAC and its partner agencies piece together intelligence from a range of sources to develop a picture of criminal activities and networks. Many partner agencies – including the Australian Federal Police, Australian Crime Commission and Australian Taxation Office (ATO) – have access to AUSTRAC SMRs, and approximately 30 per cent of SMRs submitted by the sector over a two-year period were referred to, or requested by, partner agencies for further analysis and investigation.

SMRs SUBMITTED BY SUPERANNUATION FUND TRUSTEES

294 Number of SMRs submitted

$22.3M Total value of SMRs

49 Number of superannuation fund trustees submitting at least 1 SMR

5 Number of superannuation fund trustees submitting half of the total SMRs

1 March 2014 to 29 February 2016

Common misconceptions about suspicious matter reporting

Some superannuation funds may believe that submitting an SMR could lead to criticism that the fund has done something wrong or has weak controls. This is not correct and in fact, reporting SMRs is viewed by AUSTRAC as evidence that a fund is likely to have effective AML/CTF systems and controls. Given the size of superannuation holdings and the level of criminal activity in the sector, it is likely that all funds would be exposed to potential suspicious matters. Low levels of reporting compared to industry peers may be an indicator of an ineffective AML/CTF program.

A second misconception is that funds should not submit an SMR unless they have complete and comprehensive details of the suspected criminal activity. This is not the case.

A partially completed SMR from one fund can be linked to other SMRs and other intelligence sources, helping AUSTRAC build more comprehensive financial intelligence. The reporting requirements and templates are designed to accommodate reportable matters that may not necessarily involve the complete knowledge of a matter.

A third misconception is that superannuation fund trustees should only report suspicions directly relating to transactions associated with ML/TF. Again, this is not the case. Superannuation fund trustees should also report suspicious matters associated with a range of financial criminal activity and predicate offences, including fraud, corruption and tax evasion.

Further information about SMRs can be found in the AUSTRAC compliance guide. (www.austrac.gov.au/businesses/obligations-and-compliance/austrac-compliance-guide)

CRIMINAL THREAT ENVIRONMENT

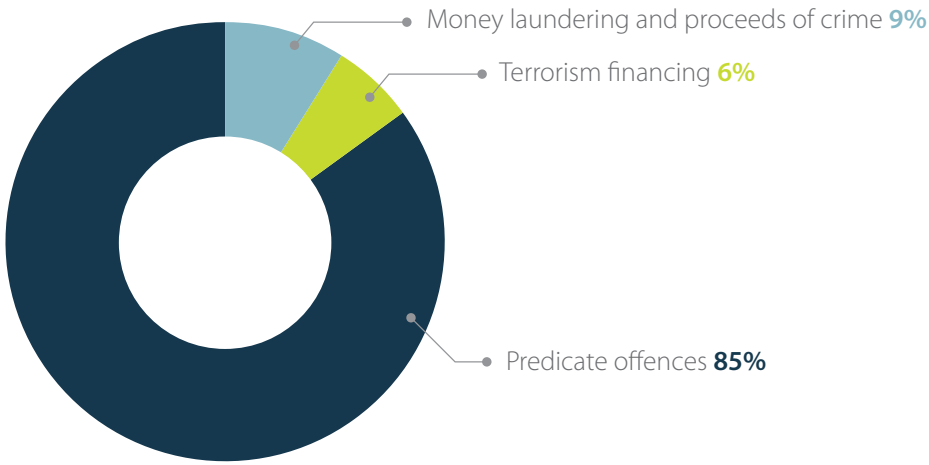
The criminal threat environment refers to the extent and nature of ML/TF and the relevant predicate crimes in an industry sector. The superannuation sector is faced with a variety of criminal threats ranging from opportunistic offences to complex crimes using sophisticated tactics and methods. Intelligence agencies have determined that organised crime groups are targeting the superannuation sector in Australia – a view shared by the superannuation funds and industry experts engaged for this risk assessment. Many funds reported significant organised crime attacks in recent years, triggering the need to enhance detection and mitigation strategies. Some funds believed that organised crime groups were moving through the sector to target funds with weak AML/CTF systems and controls.

Superannuation fund trustees reported a variety of suspected criminal offences in their SMRs during the two-year sample period. These have been grouped into three broad categories in the chart below.

MONEY LAUNDERING AND PROCEEDS OF CRIME

Superannuation fund accounts offer a means for criminals to attempt to legitimise the proceeds of crime and integrate this money into the financial system. One fund noted that patient criminals would be willing to 'park' the proceeds of crime into their funds to secure long-term capital gains.

SUSPICIOUS MATTER REPORTING BY SUSPECTED OFFENCE TYPE



In the two-year sample period, 26 SMRs (nine per cent) nominated money laundering or proceeds of crime as the most likely offence. Some common themes included:

- large contributions into superannuation accounts, followed soon after by benefit withdrawal requests
- unusually large and/or regular contributions that did not match the financial profile of the member
- members making a series of structured contributions or withdrawals under $10,000 in an attempt to avoid detection.

One fund was aware that the proceeds of corruption had been deposited into a member account. The fund was cooperating with the relevant authorities in relation to the matter.

TERRORISM FINANCING

Terrorism financing is a small but emerging and serious threat for the superannuation sector, particularly in relation to FTFs. Individuals seeking to travel to a conflict zone as an FTF often use their own money and resources to finance their travel, equipment and activities.

Self-funding can include attempts to access superannuation savings early. There is evidence that some FTFs have rolled over payments from APRA-regulated superannuation funds to SMSFs, with the money ultimately being used for terrorism financing. Fighters may also be supported by family or others in their community who are accessing their superannuation savings legitimately.

In the two-year sample period, 19 SMRs (six per cent) related to potential terrorism financing. These reports were submitted by nine superannuation funds, in relation to amounts worth $259,790 in total. While small in number, some of these SMRs were assessed by AUSTRAC as highly likely to be related to terrorism financing, and referred to law enforcement and national security agencies for further investigation.

Terrorism financing SMRs were most frequently reported as a result of a member's name appearing in media reports of Australian FTFs or in relation to counter-terrorism operations. In addition to detailing assets currently held (and frozen), some SMRs provided a useful narrative of events which showed attempts to access superannuation by claiming financial hardship provisions.

SMRs from superannuation fund trustees in relation to terrorism financing and FTFs are of significant intelligence value to AUSTRAC and national security partner agencies.

PREDICATE OFFENCES FOR ML/TF

A range of predicate offences for ML/TF were reported by the superannuation sector, accounting for 249 of the SMRs (85 per cent) submitted during the sample period. By far the most significant predicate offence is fraud,[2] including cybercrimes, illegal early releases and falsifying documents. A range of other suspicious matters, including potential tax evasion, unusual account activity, unusually large transfers and unauthorised account transactions, were also reported.

2 Many predicate offences create proceeds of crime. When proceeds of crime are transferred to or from a member's account, the criminal is effectively engaging in money laundering. Reporting entities often report the predicate crime in the SMR rather than ML, which is appropriate. This is likely to partially explain the smaller number of SMRs that specify ML as the primary suspected offence.

FRAUD AND CYBERCRIME

Many suspected offences reported by superannuation funds to AUSTRAC – particularly fraud cases – involve some form of cybercrime. Most funds consulted by AUSTRAC saw cybercrime as the single biggest threat they faced, with many funds noticing regular – even daily – hacking attempts. Hacking provides criminals with the data they need to breach the defences that superannuation providers have in place. One large fund noted that cyber-enabled fraud attempts often started with small-scale attempts to find weaknesses in a fund's procedures and systems. Once a weakness was established, the fund was subject to 'mass waves of attack' from a number of fraudsters.

It is AUSTRAC's assessment that organised crime groups are conducting sophisticated online attacks on superannuation funds, and are likely to continue seeking out weaknesses and vulnerabilities in the sector. Although most criminal activity in the superannuation sector is based domestically, there has been involvement by foreign criminal entities in the cyber domain.

Criminals engaged in cybercrime activities in the superannuation sector use a range of methods and techniques, including:

- accessing members' emails and social media accounts to obtain personal information to satisfy identity checks and access members' superannuation accounts
- hacking into members' superannuation accounts to change contact and payment details, then waiting before trying to move money, to avoid detection by the fund
- using social media to determine when a member leaves the country (and is therefore unlikely to be monitoring their account) to make changes to a member's superannuation account
- using the bank account of an unwitting third party to transfer money stolen from a member's superannuation fund into the hands of overseas-based criminals.

Complex criminal activity targeting a superannuation account

The following example was provided by a superannuation fund that experienced a significant cyber enabled fraud attack on a post-preservation account.

An overseas-based organised crime group hacked into a fund member's home computer and had access to all personal details, emails, banking details, travel plans and other information. It also monitored transactions from the individual's superannuation fund.

When the member went overseas for a holiday, the crime group made an online request from the member's email address for a variation of payment, and diverted the member's Australian phone number to an overseas number. The request was made soon after the fund had created a new online functionality for members to change their payment amounts and the frequency of payments.

The online request triggered the fund's 'member call back' control mechanism to verify that the member had made the request. When the fund's call centre staff called the member, the phone displayed the member's Australian home telephone, so they did not realise that they had called an overseas phone number.

The fraudster was able to impersonate the member and pass the customer verification procedures. The fraudster made changes to the payment amount stating that they required a one-off lump sum payment and would then revert to the normal pattern of payments. The one-off lump sum payment was subsequently made to the member's bank account.

Before the criminal group could arrange for the money to be sent offshore, the member became aware of unusual transactions and changes to their bank account and called the superannuation fund. Fortunately, the lump sum payment was frozen in their bank account and the member did not lose their savings. The fund worked closely with the state police on the investigation of the attempted theft.

FRAUD - ILLEGAL EARLY RELEASE

Attempts to gain illegal early release[3] of superannuation was commonly cited by funds in discussion with AUSTRAC as a significant threat, and was one of the most common issues described in SMRs from the sector. Many funds reported receiving requests to rollover funds into SMSFs to secure illegal early release.

Many SMRs related to members attempting to make multiple claims of financial hardship, in violation of provisions that limit the amount that can be released before preservation age to $10,000 per annum. Funds observed members withdrawing the maximum amount from their fund, then rolling over the remaining balance into a new fund and submitting a new request for early release. The requirement to action rollover requests within three days adds an additional vulnerability, as it limits the extent to which funds can identify potentially suspicious behaviour.

Further information on illegal early release and illegal superannuation schemes can be found on the ATO website (www.ato.gov.au/Individuals/Super/In-detail/Withdrawing-and-paying-tax/Illegal-super-schemes---beware-of-offers-to-withdraw-your-super-early/)

FALSIFYING DOCUMENTS

Many SMRs were in relation to falsified or altered documentation, either by a member to support a fraudulent claim, or by an agent attempting to gain unlawful access to member accounts.

Some common tactics observed in cases of falsified documents included:

- falsified or altered letters purportedly from the Department of Human Services (DHS) in support of financial hardship claims
- falsified birth certificates in attempts to gain early access to superannuation
- falsified death certificates in attempts to illegally gain access to superannuation
- use of the same Justice of the Peace to certify false documents for different members, suggesting the involvement of a scheme promoter.

Some SMRs described criminals' use of falsified identity documents – including fake certification details – to satisfy proof of identity. The criminal would then change the contact details for the member (such as their email address), and request a withdrawal. In several cases, the fund only learned of the fraud after being contacted by the member when they enquired about the withdrawal. Investigation proved these identity documents were forgeries.

New members

One fund observed that when they receive a potentially fraudulent application form for a new member, there are often anomalies with how the applicant established the account. For example, over a brief period they may apply to create several accounts, often with the same or similar name and date of birth details.

TAX EVASION

Based on SMRs submitted to AUSTRAC, superannuation funds do not appear to be a significant vehicle for tax evasion. Nineteen SMRs (six per cent) in the sample period were submitted relating to suspected tax evasion offences, with some relating to money laundering offences.

The most common grounds for suspicion in these reports were:

- a member was conducting business activities that they were not reporting to the ATO
- unusual account activity, such as a member making large deposits over a short period, suggesting tax avoidance
- members and/or their agents attempting to misrepresent information, such as evidence of their date of birth, to gain a tax advantage.

3 Superannuation can only be released before preservation age in limited circumstances, including financial hardship, compassionate grounds, death benefit payments, total and permanent disablement, income protection and trauma payments.

VULNERABILITIES

Vulnerability refers to the characteristics of an industry sector that make it vulnerable to criminal exploitation. This includes customer types, products and services, delivery channels and the foreign jurisdictions with which it deals. With some $1.26 trillion in assets,[4] the superannuation sector contains numerous features that make it vulnerable to criminal exploitation.

CUSTOMERS

The risk profile of superannuation funds is impacted by the compulsory nature of superannuation. While the sector has relatively simple customer types (mostly individuals), it has a very large customer base. Moreover, superannuation funds cannot reject membership applications, nor can they exit high risk members.[5]

INDIVIDUALS

Most SMRs lodged by superannuation funds in the sample period were in relation to an individual member of the fund – in some cases as the victim of a crime and in other cases as the suspected perpetrator. These included situations in which the fund deemed the behaviour of the member to be suspicious, or scenarios where the member's account had been compromised and subjected to attempted fraud.

With some 28 million superannuation accounts in APRA-regulated superannuation funds in Australia,[6] many funds advised that member disengagement was one of their most significant risks. This was particularly the case for younger members who were still many years from preservation age, and therefore less likely to notice fraudulent activity on their superannuation account. Many funds consulted by AUSTRAC reported attempting to improve the level of engagement with their members, including through developing new apps and real-time online notification of contributions or payments.

Post-preservation accounts present the greatest opportunities for criminal abuse, as once a member reaches preservation age, they can make transactions to and from their superannuation account, much like a bank account. This increases the likelihood of the account being subject to attempted fraud, and presents a possible ML channel.

Funds also observed that older members were particularly vulnerable to scams. For example, funds reported cases in which older members would receive a phone call from a scammer claiming to be a government official. The scammer would convince the member to provide personal and sensitive details, which the scammer could then use to gain access to the member's account.

AGENTS AND FINANCIAL ADVISERS

Only 14 SMRs (five per cent) in the sample period were in relation to agents of customers. Of these, some were relatives trying to fraudulently obtain a family member's benefits. Others related to financial advisers, with one fund consulted by AUSTRAC viewing fraudulent financial hardship claims made through financial advisers as an emerging trend and significant vulnerability.

Some funds were aware of financial advisers impersonating a member and calling funds directly. While in many instances this was to avoid the additional work associated with involving the member, some funds were also aware of advisers who were attempting to steal from members.

Some funds also highlighted the possibility of rollover schemes being promoted to individuals by unscrupulous advisers, with the members potentially unaware of the illegality of the transaction. One fund advised it had provided training to its staff to recognise this behaviour.

Funds also reported cases in which criminals hacked into members' webmail accounts and emailed instructions to the member's financial adviser to make a superannuation transaction purportedly on behalf of the member.

---

4 Australian Prudential Regulation Authority, *Quarterly Superannuation Performance Statistics December 2015*.

5 With the exception of corporate superannuation funds that may apply eligibility rules for membership.

6 Australian Prudential Regulation Authority, *Annual Superannuation Bulletin Statistics June 2015*.

POLITICALLY EXPOSED PERSONS

PEPs are considered higher risk customers. All reporting entities are required under the AML/CTF Rules to screen their customer base for PEPs. Following changes introduced in 2014 to the definition of PEPs in the AML/CTF Rules, reporting entities are now required to conduct screening for domestic, as well as foreign, PEPs. During discussions with AUSTRAC, several funds noted they had identified many PEP customers as a result of these changes. But some funds and industry experts noted it was likely that some were still not aware of, or did not understand, this requirement.

Due to the compulsory nature of superannuation, it is likely that a large number of domestic PEPs will have accounts with APRA-regulated funds; however, very few SMRs from superannuation funds relate to PEPs. One fund noted that most PEPs in its fund were in a defined benefits scheme, which is a lower risk product. It is unlikely that APRA-regulated superannuation funds would have accounts for foreign PEPs. Further information about obligations relating to PEPs can be found on the AUSTRAC website (www.austrac.gov.au/part-b-amlctf-program-customer-due-diligence-procedures).

SOURCE OF FUNDS AND WEALTH

Fund contribution payments received from an employer carry a low level of risk as the source can be readily established; however, payments direct from a member present a higher risk because of the potential difficulties in determining their source. Many funds consulted by AUSTRAC identified assessing a member's source of funds or wealth as a challenge.

Rollovers into a superannuation fund from an SMSF also create an avenue for ML in the sector. The origins of this money is difficult to determine, but can include the proceeds of crime.

One fund advised that its call centre had started contacting members in relation to some after-tax (voluntary) contributions, to assist in determining whether the contribution was legitimate or suspicious.

Employer risks

Several funds noted that employers (in their capacity as payers of superannuation contributions) were a potential risk for illegal activity, with one fund saying that understanding employer risk was an industry 'blind spot' and needed further attention.

In some cases, funds reported employers committing fraud, such as through registering fake employees, creating a potential money laundering channel. While under the AML/CTF Act the employer is not the customer of the fund, an SMR may be lodged under section 41 in relation to the fictitious employee, which may lead to scrutiny of the employer's conduct.

In other cases, employers were the target of fraud. One fund was aware of members who were defrauding their employers, then putting the proceeds into their own superannuation accounts. In this scenario the fund could submit an SMR based on the reasonable suspicion that the information may be relevant to investigation of, or prosecution of a person for, an offence against a law of the Commonwealth or a state or territory. In discussions with AUSTRAC, some funds highlighted the challenges associated with having limited visibility over employers.[7] Some reported conducting a variety of due diligence and analytics work on employers before they were accepted or formally registered with the fund. For example, one fund checks ABNs, conducts monthly analysis for employers using common addresses, and checks for employers who have an unusual number of employees without a tax file number.

7 The risk posed by an employer may be lower for a corporate fund.

PRODUCTS AND SERVICES

Superannuation products and services present various levels of vulnerability. Lower risk products include eligible rollover funds and defined benefits funds where they do not allow members to make contributions. Higher risk products include accumulation funds and post-preservation accounts, which allow relatively easier movement of funds.

There are several factors that limit the vulnerability of most superannuation fund products for money laundering These include:

- conditions and restrictions on when money can be moved to and from superannuation accounts
- taxes levied on excess/voluntary contributions
- the high level of visibility of transactions by the ATO
- the relatively low level of customer anonymity; and the non-transferability of superannuation accounts between people.

These factors do not, however, reduce the vulnerability of these products to fraud.

OUTGOING TRANSACTIONS

Outgoing transactions from the superannuation sector – such as payments to members and rollovers to other funds – are large in scale and volume. These factors present significant vulnerabilities, particularly in relation to fraud. In 2015, benefit payments from APRA-regulated funds totalled $62.8 billion.[8]

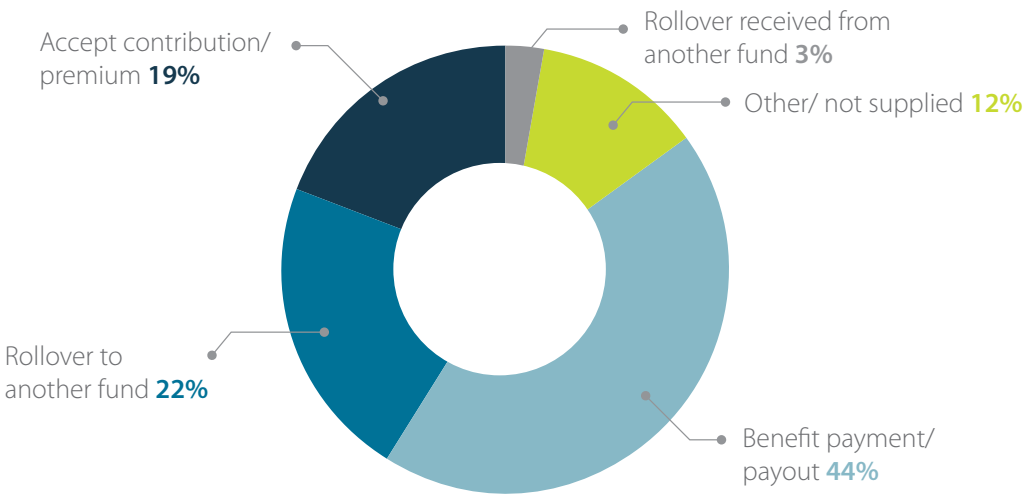
Almost two-thirds of SMRs in the sample period related to outgoing transactions:

- 128 SMRs (44 per cent) related to benefit payments
- 66 SMRs (22 per cent) related to rollovers to another fund.

Most of these SMRs detailed attempted fraud and/or suspected illegal early release of superannuation savings, with a small number in relation to terrorism financing. These are detailed in the 'Criminal threat environment' section of this risk assessment.

Attempted fraud is often detected by superannuation funds when payments are released, as this is the stage when the identity of the member must be verified, as per requirements under the AML/CTF Act.

NUMBER OF SUSPICIOUS MATTER REPORTS BY TRANSACTION TYPE



8 Australian Prudential Regulation Authority, *Quarterly Superannuation Performance Statistics December 2015*.

Mitigating the threat of illegal early release

Some funds consulted by AUSTRAC were mitigating the risks associated with illegal release through a range of controls, including:

- not making early release payments to agents
- calling members to ask questions in relation to rollovers to other funds
- only making cheque payments to registered addresses (not PO Box addresses), including when making rollover payments to another fund
- only processing hardship claims if members consented to the fund seeking information from previous funds
- asking members to authorise fund access to DHS information to verify if members were receiving applicable income support.

Forum shopping

Some funds had observed members engaging in 'forum shopping' to identify which funds had weaker AML/CTF controls. For example, a member would make an application for early release due to hardship, and if unsuccessful, they would roll over their account to a new fund, and make another hardship application there. Although the ATO would be advised of these payouts, individual funds have no visibility of prior attempts by a member to access an early release, due to the tipping off provisions in the AML/CTF Act.

INCOMING TRANSACTIONS

Receiving money into a superannuation fund account presents a relatively lower risk than making outgoing payments to members and rollovers, particularly in relation to fraud. However, some incoming transactions pose higher levels of risk, such as voluntary (non-concessional) contributions from members, because the source of these funds is more difficult to determine. These contributions could include the proceeds of crime derived from tax evasion or corruption, and may be part of the ML process. This risk is elevated by the fact that funds are required to accept all contributions made by employers and members.

Another significant challenge for the sector is the scale and volume of transactions. In 2015, contributions to APRA-regulated funds (including employer and member contributions) totalled $103.9 billion.[9]

Funds generally do not perform a customer identification procedure at this point due to the exemption in section 39 of the AML/CTF Act. Despite this limitation, several funds are submitting SMRs on incoming contributions.

In the sample period, 64 SMRs (22 per cent) were in relation to incoming transactions:

- 56 SMRs (19 per cent) related to the acceptance of a contribution or premium
- eight SMRs (three per cent) related to rollovers received from another superannuation fund.

DELIVERY CHANNEL

The growing reliance on online delivery of superannuation products and services makes the sector vulnerable in a number of ways.

Superannuation funds have very limited face-to-face contact with their members. The frequent use of email communication between funds and customers creates a favourable environment for cybercrime.

A clear trend in many funds is an increased emphasis on the 'member experience'. That is, developing new and novel capabilities that empower members to make changes online to their profiles, contact details, payment frequency and payment amount. Without robust safeguards in place, these types of changes could unintentionally create new and significant vulnerabilities.

9 Australian Prudential Regulation Authority, *Quarterly Superannuation Performance Statistics December 2015*.

Using technology to mitigate risk

Several funds and fund administrators have developed, or are developing, data analytics capabilities to detect unusual or suspicious activity. One fund is currently developing a real-time sophisticated digital fraud protection framework. This includes data matching and analytics on a range of data and information sources including IP addresses, device recognition software, the incidence and type of changes made to member details, and member calls to the call centre. These checks, balances and frameworks are being designed to identify potentially suspicious matters in real time.

After an attempted online attack from an organised crime group, one fund instituted a range of new controls. The fund placed restrictions on pension payment variation requests and refreshed the existing awareness training program for staff to assist in identifying the risks associated with the attack. The fund also submitted a paper to the board on lessons learned from the attack, identified key gaps in their controls, and recommended actions for improvement.

FOREIGN JURISDICTION

Superannuation funds tend to have minimal exposure to jurisdiction risk, as most have only a very small number of overseas-based members; for example, when an Australian citizen is working overseas for an Australian organisation.

However, jurisdiction risk can be an issue in relation to departing Australia superannuation payments (DASP). One fund advised AUSTRAC that it only provides DASPs by electronic funds transfer to low- and medium-risk countries, and only when an AUD cheque could not be presented in that country. Some funds only make DASPs to domestic bank accounts and do not make payments to overseas accounts or addresses.

Fourteen SMRs (five per cent) in the sample period referred to countries other than Australia, several of which were higher risk jurisdictions. The total value of these reports was $1.5 million. All but one of these SMRs referred to outbound transactions.

USE OF CASH

Cash transactions are generally a significant indicator of money laundering placement risk, though these appear to be extremely uncommon for the superannuation industry. Of the SMRs analysed, only four (one per cent) mentioned the use of cash transactions. Most were reported on the basis that they appeared to involve suspicious behaviour or unusual account activity.

There appears to be a trend among funds to limit or cease the acceptance of cash payments to the superannuation fund trustee's premises. This is due to the high-risk nature of cash, as well as the requirements of maintaining cash-handling facilities. This is reflected in the data submitted in threshold transaction reports (TTRs) by superannuation fund trustees.[10]

TTRs SUBMITTED BY SUPERANNUATION FUND TRUSTEES

28 Number of TTRs submitted

$782,933 Total value of TTRs

$27,962 Average value of TTRs

5 Number of superannuation fund trustees submitting at least 1 TTR

1 March 2014 to 29 February 2016

10 All reporting entities must submit a TTR for transactions involving physical currency or e-currency valued at AUD10,000 (or foreign equivalent) or higher.

OPERATIONAL VULNERABILITIES

Superannuation funds and industry experts consulted for this report also highlighted some common internal and operational vulnerabilities.

Data security was identified as a critical vulnerability, as funds continue to move towards digitising their internal operations, such as through cloud services and offshore service providers.

As well as encouraging members to keep their personal data secure, funds should also consider risks posed from employees, fund administrators, financial planners and other outsourced providers who can access sensitive information. This should also apply to contractors, including those based overseas, who may be engaged to assist with product design and digital strategies, and may have access to member information. Funds should have controls in place to audit internal access to members' information to prevent misuse and fraud.

Fund employees in particular may be in positions where they could facilitate or execute money laundering, or a predicate crime such as fraud. One fund suggested in discussions with AUSTRAC that post-preservation accounts are most vulnerable to internal fraud because of the ability to withdraw a lump sum payment.

Outsourcing fund administration

When outsourcing operations relating to superannuation accounts, the fund trustee remains responsible for meeting obligations under the AML/CTF Act. The common practice of outsourcing fund administration requires trustees to remain highly engaged with their administrators to ensure effective AML/CTF controls are in place, including the capacity to identify and report SMRs.

Trustees should have a clear understanding of the processes used by their administrator and clearly communicate their own requirements and procedures. They should also follow up on implementation to ensure their requirements are consistently met.

One fund reported that it organised workshops with its administrator to go through every SMR trigger being used, to ensure the trustee understood the triggers and how they were being applied. As part of this exercise, triggers that were no longer relevant to the fund were removed and new ones were added.

For administrators, constraints in the AML/CTF Act around tipping off were identified as a vulnerability. An administrator working for many funds could identify suspicious behaviour by a member in multiple funds but cannot provide this holistic perspective to individual fund clients, thereby limiting the capacity to understand and mitigate risks posed by members.

AML/CTF SYSTEMS AND CONTROLS

It is highly likely that there is significant under-reporting and non-reporting of suspicious matters across the superannuation industry, which would indicate that internal controls and compliance cultures need to be strengthened. This view is strongly supported by various superannuation funds and industry experts that provided input to this report.

Reporting of SMRs was concentrated among a small group of funds, with only five superannuation funds accounting for over half of the total reports received in the sample period. In addition, AUSTRAC would expect to see suspicious matter reporting from the sector that better reflects the value of money moving through the superannuation system, the number of superannuation accounts, and the capability of criminals to target the sector (including concerns raised by industry). The various misconceptions about the submission of SMRs outlined in this assessment may contribute to deficiencies in reporting.

One significant impact of this is that AUSTRAC and its partner agencies lack the information needed to develop a comprehensive and accurate picture of the criminal threat to the sector. This hinders the government's ability to investigate and respond to criminal activity.

AUSTRAC notes, however, that during consultation for this assessment, a number of AML/CTF compliance officers showed a very high level of awareness and understanding of the threat environment and vulnerabilities facing their funds. In several cases, these officers described sophisticated mitigation responses that had been implemented – or were in the process of being implemented – by their fund. One fund talked about its commitment to engage and educate frontline staff so they were better able to identify suspicious behaviour. As a result, there was a significant increase in referrals of potentially suspicious matters. Other mitigation responses are detailed throughout this assessment.

Some funds reported that their boards were highly accessible, engaged and aware of the risks associated with ML/TF and the various predicate offences. However, both funds and industry experts were concerned that this level of accessibility and board engagement may not be consistent across the sector.

CONSEQUENCES

Consequence refers to the potential impact or harm that ML/TF and predicate crimes may cause. Money laundering in the superannuation sector has consequences for superannuation fund members, individual superannuation funds and the sector as a whole, and the broader Australian economy. Terrorism financing, though small in the sector, has very significant consequences, including sustaining terrorist groups, and potentially enabling terrorist acts in Australia and overseas.

SUPERANNUATION FUND MEMBERS

The direct financial cost to the member of ML or predicate crimes may be mitigated as there are compensation arrangements applicable to APRA-regulated super funds in the case of fraud or theft. However, there are still some financial and indirect consequences for members, including:

- undetected losses from accounts of members, including disengaged members
- reduced retirement benefits
- emotional distress
- loss of confidence in the superannuation system.

SUPERANNUATION FUNDS AND THE SUPERANNUATION SECTOR

The severity of consequences will differ between funds depending on the extent to which they can understand and assess ML/TF risks, identify and submit SMRs, and have effective internal controls and strategies in place to combat the various criminal threats outlined in this assessment.

As such, the most significant consequences of ML and associated predicate crimes will likely be borne at the individual fund level. This could include:

- continual erosion of the financial performance of the fund due to crime-related losses
- increased fraud insurance premiums
- increased costs associated with combating criminal attacks
- increased administrative costs in reviewing potentially thousands of transactions upon the discovery of a fraudulent/criminal transaction
- increase to the Operational Risk Financial Reserve
- potential adverse impact on earnings
- reputational damage to a fund following an attack, resulting in decreased membership and damage to the brand
- public relations costs associated with regaining community trust
- increased regulatory action.

AUSTRALIAN ECONOMY

Financial crimes in the superannuation sector have the potential to impact the broader Australian economy, including:

- loss of savings from stolen superannuation holdings
- widespread loss in confidence in the superannuation system, with flow-on implications for Australians' retirement holdings
- undetected criminal activity, thereby providing a safe haven for the proceeds of crime
- increased reliance on the Government Age Pension.

NATIONAL SECURITY AND INTERNATIONAL CONSEQUENCES

Terrorism financing, though currently small in the superannuation sector, is judged to have moderate consequences, both in Australia and overseas, including:

- sustaining and enabling the activities of Australian FTFs
- potentially enabling terrorist acts both in Australia and overseas
- harming Australia's global image.

CONCLUSION

The superannuation sector in Australia is faced with a serious and multifaceted criminal threat environment. The volume and value of money moving through the sector, and the number of member accounts at the national level, make it an attractive and lucrative target for both opportunistic criminals and well-resourced organised crime groups. The threat is exacerbated by increasingly sophisticated cybercrime capabilities. Terrorism financing activity presents a challenge for the industry and government given the significant consequences that can occur with small amounts of funds. AUSTRAC assesses that criminal entities will continue to exploit vulnerabilities specific to the superannuation sector and target funds with weaker detection and control mechanisms.

AUSTRAC believes that significant opportunity exists for superannuation funds to leverage this assessment and to expand their suspicious matter reporting and strengthen internal controls against financial crime. AUSTRAC will continue to support the sector by providing advice and guidance on ML/TF risks. In addition, AUSTRAC will monitor SMR trends after the publication of this assessment to determine if reporting levels have increased across the sector, and this information will inform future intelligence-led compliance activities.

FEEDBACK

AUSTRAC is committed to continual improvement and values your feedback on our products. We would appreciate notification of any outcomes associated with this report by contacting us via riskassessments@austrac.gov.au

APPENDIX A

RISK ASSESSMENT METHODOLOGY

The methodology below covers 26 risk factors across three categories – criminal threat environment, vulnerabilities and consequences. Each risk factor was assessed as either low, medium or high, as per the table below. These assessments were based on quantitative and qualitative intelligence inputs, including analysis of SMR and other reporting data, intelligence assessments from partner agencies, and feedback from industry.

For **criminal threat environment**, six risk factors were considered – each was given equal weight. The average of these six ratings gave an overall rating for threat.

For **vulnerabilities**, there were 16 risk factors. These were grouped into eight subsections – customers, source of funds and wealth, products and services, delivery channel, foreign jurisdiction, use of cash, operational vulnerabilities, and AML/CTF systems and controls. The average of these eight subsections gave an overall rating for vulnerabilities.

For **consequences**, four risk factors were considered – each was given equal weight. The average of these ratings gave an overall rating for consequences.

CRIMINAL THREAT ENVIRONMENT

LOW	MEDIUM	HIGH
Unsophisticated tactics and methods used	Some sophisticated tactics and methods used	Highly sophisticated tactics and methods used
Low volume of cyber-enabled criminal activity	Moderate volume of cyber-enabled criminal activity	High volume of cyber-enabled criminal activity
Minimal targeting by serious and organised crime groups and/or foreign criminal entities	Some targeting by serious and organised crime groups and/or foreign criminal entities	Widespread targeting by serious and organised crime groups and/or foreign criminal entities
Low volume of money laundering	Moderate volume of money laundering	High volume of money laundering
Very few instances of raising and/or transferring funds for terrorism financing	Some instances of raising and/or transferring funds for terrorism financing	Many instances of raising and/or transferring funds for terrorism financing
Low volume and/or limited variety of other offences	Moderate volume and/or some variety of other offences	High volume and/or large variety of other offences

VULNERABILITIES

LOW	MEDIUM	HIGH
Customers		
Simple customer types, mostly individuals	Mixture of customers types, with some complex companies and trusts	All customer types represented, including large numbers of highly complex companies and trusts
Minimal involvement of agents acting for customers	Moderate involvement of agents acting for customers	Significant involvement of agents acting for customers
Small customer base	Medium-sized customer base	Very large customer base
Very few politically exposed persons (PEPs)	Some politically exposed persons (PEPs)	Many politically exposed persons (PEPs)
Source of funds and wealth		
Source of funds/wealth can be readily established	Some difficulty in establishing the source of funds/wealth	Source of funds/wealth difficult to establish
Products and services		
Product/service does not allow a customer to remain anonymous (ownership is transparent)	Product/service allows a customer to retain some anonymity (ownership can be obscured)	Product/service allows a customer to remain anonymous (ownership is opaque)
Small volume of transactions	Moderate volume of transactions	Large volume of transactions
Movement of funds cannot occur easily and/or quickly	Movement of funds can occur relatively easily and/or quickly	Movement of funds is easy and/or quick
Transfer of ownership of product cannot occur easily and/or quickly	Transfer of ownership of product can occur relatively easily and/or quickly	Transfer of ownership of product is easy and/or quick
Delivery channel		
Regular face-to-face contact, with minimal online/telephone services	Mix of face-to-face and online/telephone services	Predominantly online/telephone services, with minimal face-to-face contact
Foreign jurisdiction		
Very few or no overseas-based customers	Some overseas-based customers	Many overseas-based customers
Transactions rarely or never involve foreign jurisdictions	Transactions sometimes involve foreign jurisdictions, or a high-risk jurisdiction	Transactions often involve foreign jurisdictions, or high-risk jurisdictions

LOW	MEDIUM	HIGH
Use of cash		
Provision of product/service rarely involves cash, or involves cash in small amounts	Provision of product/service often involves cash, or involves cash in moderate amounts	Provision of product/service usually involves cash, or involves cash in very large amounts
Operational vulnerabilities		
There are very few operational factors that make the sector susceptible to criminal activity	There are some operational factors that make the sector susceptible to criminal activity	There are many operational factors that make the sector susceptible to criminal activity
AML/CTF systems and controls		
Sector is subject to all or most AML/CTF obligations	Sector is subject to partial AML/CTF obligations	Sector is not subject to AML/CTF obligations
At a sector level, significant systems and controls have been implemented to mitigate against criminal threats.	At a sector level, moderate systems and controls have been implemented to mitigate against criminal threats.	At a sector level, limited systems and controls have been implemented to mitigate against criminal threats.

CONSEQUENCES

MINOR	MODERATE	MAJOR
Criminal activity results in minimal personal loss	Criminal activity results in moderate personal loss	Criminal activity results in significant personal loss
Criminal activity does not significantly erode the sector's financial performance or reputation	Criminal activity moderately erodes the sector's financial performance or reputation	Criminal activity significantly erodes the sector's financial performance or reputation
Criminal activity does not significantly affect the Australian economy	Criminal activity moderately affects the Australian economy	Criminal activity significantly affects the Australian economy
TF activity has minimal potential to impact on national security and/or international security	TF activity has the potential to moderately impact on national security and/or international security	TF activity has the potential to significantly impact on national security and/or international security

www.austrac.gov.au

JULY 2016