



Australian Government

AUSTRAC

FIGHTING  
FINANCIAL  
CRIME  
TOGETHER



# AUSTRALIA'S SUPERANNUATION SECTOR

MONEY LAUNDERING AND TERRORISM FINANCING THREAT UPDATE

## COPYRIGHT

© Commonwealth of Australia 2022

All material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence ([www.creativecommons.org/licenses](http://www.creativecommons.org/licenses)).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.

The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence ([www.creativecommons.org/licenses](http://www.creativecommons.org/licenses)).



Use of the Commonwealth Coat of Arms The terms under which the Coat of Arms can be used are detailed on the It's an Honour website ([www.pmc.gov.au/government/its-honour](http://www.pmc.gov.au/government/its-honour)).

This risk assessment is intended to provide a summary and general overview; it does not assess every risk or product relevant to foreign subsidiary banks. It does not set out the comprehensive obligations under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act), the Anti Money Laundering and Counter Terrorism Financing (Prescribed Foreign Countries) Regulations 2018 (AML/CTF Regulations) or the Anti Money Laundering and Counter Terrorism Financing Rules Instrument 2007 (No. 1) (AML/CTF Rules). It does not constitute nor should it be treated as legal advice or opinion. The Commonwealth accepts no liability for any loss suffered as a result of reliance on this publication. AUSTRAC recommends that independent professional advice be sought.

## CONTACT US

If you have questions about your AUSTRAC compliance obligations, or enquiries regarding the licence and any use of this report please email [contact@austrac.gov.au](mailto:contact@austrac.gov.au) or phone 1300 021 037 (within Australia).

AUSTRAC is committed to continual improvement and values your feedback on its products. We would appreciate notification of any outcomes associated with this report by contacting AUSTRAC at [austrac.gov.au/contact-us/form](http://austrac.gov.au/contact-us/form).

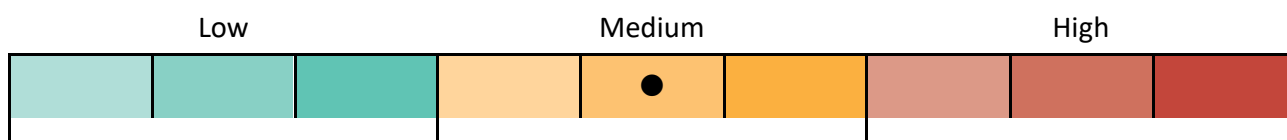
# CONTENTS

---

- EXECUTIVE SUMMARY ..... 4
- PURPOSE..... 7
- BACKGROUND ..... 8
- METHODOLOGY ..... 9
- REPORTING TO AUSTRAC..... 10
- CRIMINAL THREAT ENVIRONMENT ..... 12
  - MONEY LAUNDERING ..... 14
  - TERRORISM FINANCING..... 17
  - PREDICATE OFFENCES..... 18
  - SIGNIFICANT SHIFTS..... 24
  - EMERGING RISKS ..... 25
- APPENDIX A: GLOSSARY ..... 27
- APPENDIX B: METHODOLOGY ..... 29

# EXECUTIVE SUMMARY

## CRIMINAL THREAT ENVIRONMENT



AUSTRAC assesses the overall money laundering and terrorism financing (ML/TF) risk associated with the superannuation sector in Australia to be **medium**. This is consistent with the findings from the [\*Money Laundering and Terrorism Financing \(ML/TF\) Risk Assessment of Australia's superannuation sector\*](#) published in 2016 ('the 2016 assessment'). The superannuation sector continues to be exposed to a similar variety of threats however, the sophistication of activity associated with some offences has increased and evolved since the 2016 assessment.

This rating is based on assessments of the criminal threat environment, which refers to the nature and extent of ML/TF and other predicate offences associated with the sector.

CRIMINAL THREAT ENVIRONMENT	RISK LEVEL		CHANGE SINCE 2016
MONEY LAUNDERING		Medium	Consistent ↔
TERRORISM FINANCING		Low	Decreased ↓
PREDICATE OFFENCES		High	Increased ↑

## Money laundering

The superannuation sector continues to be exposed to medium levels of money laundering activity, however the methodologies used to facilitate this activity have increased in complexity. This includes the use of staging accounts and self-managed superannuation funds (SMSFs) to transfer value out of the financial system.

## Terrorism financing

The superannuation sector is exposed to low levels of terrorism financing threats. This assessment is based on the low and decreased number of terrorism financing-related suspicious matter reports (SMRs) submitted by the sector, intelligence holdings, feedback from partner agencies, and open-source information.

## Predicate offences

The superannuation sector has a high exposure to predicate offences, which range from a low level of sophistication to more complex activity.<sup>1</sup> Cybercrime continues to be a key enabler of offences in the sector, and has contributed to an increase in suspicious activity. The key predicate offences impacting the sector are fraud, scams and tax evasion.

## SIGNIFICANT SHIFTS AND EMERGING RISKS

SIGNIFICANT SHIFTS AND EMERGING RISKS	
DATA AS A COMMODITY	MERGER ACTIVITY
FAMILY FRAUD, ELDER ABUSE & DOMESTIC VIOLENCE	STAPLING

AUSTRAC has identified several shifts and emerging risks facing the superannuation sector that are new or have changed since the 2016 assessment. A key shift involves the targeting of data as a commodity which has seen cybercriminals targeting superannuation funds to obtain member data in bulk. Emerging risks include the increased vulnerability to family fraud, elder abuse and financial fraud associated with domestic violence.

<sup>1</sup> For the purposes of this report, a predicate offence is a criminal offence that generates proceeds of crime, or other related crimes such as identity fraud.

## IMPACTS OF COVID-19

In March 2020, the Australian Government announced assistance to support individuals and businesses to manage the economic impact of the COVID-19 pandemic. The COVID-19 early release of superannuation (ERS) scheme allowed individuals impacted by the pandemic to access part of their superannuation early.<sup>2</sup> Funds experienced a significant increase in the volume of ERS claims during this period, including under the scheme. This included an increase in the volume of claims submitted fraudulently, resulting in an increase in SMRs.

During this period, funds were exempt from conducting customer verification for payments approved by the Australian Taxation Office (ATO) when related to the COVID-19 ERS scheme.<sup>3</sup> This enabled flexibility in an existing legislative control, likely contributing to the increased attempts to fraudulently access superannuation payments.

AUSTRAC acknowledges the reporting period used in this report captures activity conducted both during and after the COVID-19 ERS scheme. This report therefore assesses the ML/TF impacts resulting from the pandemic, as well as the overall activity occurring within the sector more broadly.

<sup>2</sup> Eligible individuals were able to access their superannuation between 19 April 2020 and 31 December 2020. ATO, *COVID-19 early release of super*, <https://www.ato.gov.au/Individuals/Super/In-detail/Withdrawing-and-using-your-super/COVID-19-early-release-of-super>.

<sup>3</sup> AUSTRAC, *New customer verification AML/CTF Rule to support early release of superannuation initiative*, <https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/new-customer-verification-amlctf-rule-support-early-release-superannuation-initiative>.

## PURPOSE

This report provides information specific to Australia's superannuation sector on the ML/TF risks the sector faces at the national level. Its primary aim is to provide an update of the criminal threat environment of the sector to identify and disrupt ML/TF risks to Australia's financial system, and encourage the sector to report suspected crimes to AUSTRAC.

This report is not intended to provide targeted guidance or recommendations as to how reporting entities should comply with their anti-money laundering and counter-terrorism financing (AML/CTF) obligations. However, AUSTRAC expects Australia's superannuation sector to review this assessment to:

- inform their own ML/TF risk assessments
- review and strengthen their risk mitigation systems and controls, and
- enhance their understanding of risk in the sector.













AUSTRAC acknowledges the diversity of entities within the sector and recommends this assessment be considered according to each business' individual operations.

## BACKGROUND

In October 2016, AUSTRAC released its first *Money Laundering and Terrorism Financing (ML/TF) Risk Assessment of Australia's superannuation sector*. That report assessed the **overall ML/TF risk** to the sector as **medium**.

This report provides an update of the criminal threat environment facing the superannuation sector and assesses the current ML/TF threats, key predicate offences, and highlights notable shifts and emerging risks that are new or have changed since the 2016 assessment. This report does not assess inherent vulnerabilities or consequences of ML/TF activity, or discuss risk mitigation strategies.

### AUSTRALIA'S SUPERANNUATION SECTOR<sup>4 5 6</sup>

	2016	 	2021
 Number of funds	242		149
 Number of member accounts	28 million		21.3 million
 Total assets	\$1.3 trillion		\$2.3 trillion
 Total annual contributions	\$103.9 billion		\$127.2 billion
 Total annual benefit payments	\$62.8 billion		\$94.9 billion

The information in this report relates to superannuation funds regulated by the Australian Prudential Regulation Authority (APRA). These include corporate funds, industry funds, public sector funds and retail funds. It does not assess the risk to SMSFs, however it does refer to SMSFs where the risks are relevant to APRA-regulated funds.

<sup>4</sup> APRA-regulated superannuation entities with more than four members.

<sup>5</sup> AUSTRAC, *Money Laundering and Terrorism Financing (ML/TF) Risk Assessment of Australia's superannuation sector*, <https://www.austrac.gov.au/sites/default/files/2019-06/super-annuation-risk-assessment-WEB2.pdf>.

<sup>6</sup> APRA, *Annual superannuation bulletin – June 2021*, <https://www.apra.gov.au/sites/default/files/2022-01/Annual%20superannuation%20bulletin%20highlights%20-%20June%202021.pdf>.



## METHODOLOGY

The methodology used for this report assessed the **criminal threat environment** against six risk factors to determine an average risk rating. The criminal threat environment refers to the nature and extent of ML/TF and relevant predicate offences in a sector.

Further information on the methodology and how this was applied to the sector is in Appendix A.

The risk ratings in this assessment were informed by five main intelligence inputs:

- Over 1,700 SMRs submitted by the sector between 1 September 2020 and 31 August 2021, including a sample of 529 SMRs on which detailed analysis was undertaken (the **SMR sample**).<sup>7</sup>
- A comprehensive review of 25 AUSTRAC and partner agency intelligence reports produced between 1 January 2019 and 31 August 2021 (the **IR review**).<sup>8</sup>
- Open source information, including public-facing information produced by government agencies, regulators, academic institutions, reporting entities and the media.
- Feedback and professional insights offered during correspondence with a range of reporting entities in the sector, and consultations with partner agencies and industry experts.
- Information obtained in response to a questionnaire issued to a range of reporting entities in the superannuation sector (the **questionnaire**). This questionnaire included questions regarding the criminal threat environment and various factors of ML/TF vulnerability.

<sup>7</sup> SMRs should be considered indicative of suspicious behaviour only and not conclusive in their own right. This is because reporting entities generally lack visibility of certain threat elements, for example how a customer generates suspected criminal proceeds. To ensure accuracy of ML/TF indicators (threats and vulnerabilities) outlined in the SMR sample, AUSTRAC officers manually reviewed and categorised each report.

<sup>8</sup> The number of IRs may not reflect the actual extent of criminality, and may understate the true extent of ML/TF threats and criminal misuse of the sector. This is because AUSTRAC does not have visibility of all partner agency intelligence reporting.

## REPORTING TO AUSTRAC

### SMRS SUBMITTED BY THE SUPERANNUATION SECTOR BETWEEN 1 SEPTEMBER 2020 AND 31 AUGUST 2021

Number of reporting entities: **129<sup>9</sup>**

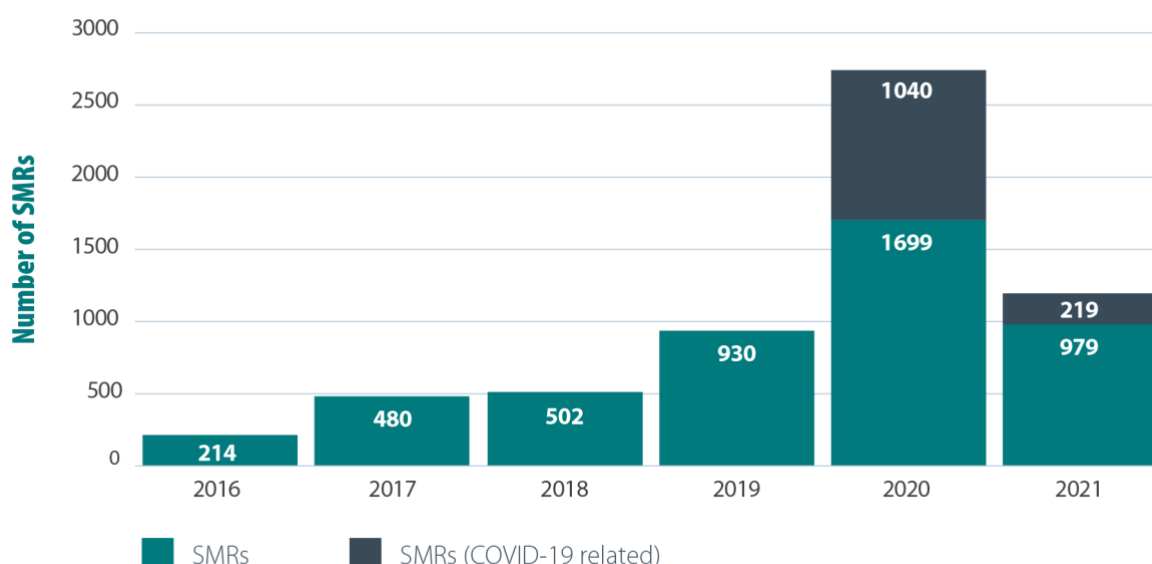
Number of SMRs: **1,783**

Value of SMRs:<sup>10</sup> **\$112,654,333**

Percentage of funds reporting at least one SMR: **50%**

Number of funds accounting for 55% of reporting: **5**

### A SHOUT OUT TO INDUSTRY: SIGNIFICANT INCREASE IN SMR REPORTING



**Figure 1: SMRs submitted by the superannuation sector between 2016 and 2021.**

The 2016 assessment aimed to increase industry awareness of ML/TF risks in the superannuation sector, and encourage reporting of suspicious transactions. AUSTRAC acknowledges the impact of COVID-19 on suspicious activity, however the overall volume and detail of industry reporting to AUSTRAC has also increased significantly since the release of the 2016 assessment and related outreach with the sector. AUSTRAC acknowledges the efforts of the superannuation sector for their positive response and encourages reporting entities to continue reporting suspicious matters.

### SMRs play a crucial role in law enforcement

Under the *AML/CTF Act*, reporting entities have an obligation to report suspicious matters to AUSTRAC. A reporting entity must submit an SMR under a number of circumstances, including if they

<sup>9</sup> A reporting entity may be trustee for more than one superannuation fund.

<sup>10</sup> Caution should be exercised when interpreting the recorded value in SMRs. The recorded value may not necessarily relate to suspected criminal misuse or terrorism financing, and may include values of transactions that occurred outside the reporting period. This is because a reporting entity may not form a suspicion and submit an SMR until multiple transactions are conducted – some of which may have occurred outside the reporting period.

suspect on reasonable grounds that information they have concerning a service they are providing, or will provide, may be relevant to the investigation or prosecution of a crime.

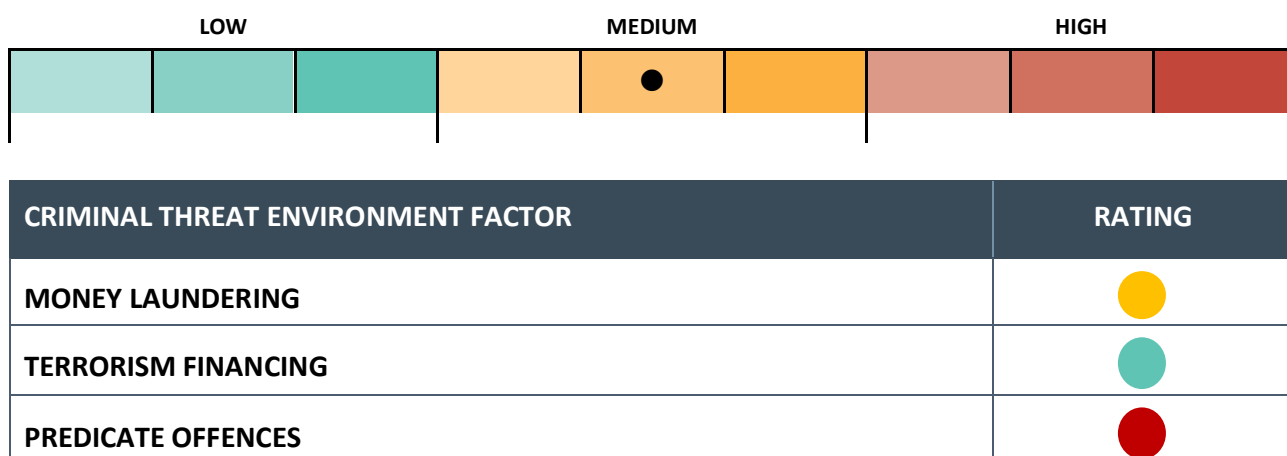
SMRs provide valuable intelligence to AUSTRAC. Working with its partner agencies, AUSTRAC pieces together intelligence from a range of sources to develop a picture of criminal activities and networks. Many of AUSTRAC's partner agencies – including the Australian Federal Police (AFP), the Australian Criminal Intelligence Commission (ACIC) and the Australian Taxation Office (ATO) – have access to SMRs to generate investigative leads and conduct further analysis and investigation. High-quality, accurate and timely SMRs give AUSTRAC and our partners the best chance to detect, deter and disrupt criminal and terrorist activity.

### **What happens after AUSTRAC receives an SMR?**

When an SMR is submitted to AUSTRAC, it is processed to detect crime types and surface high priority matters for immediate analysis. Reports and alerts are then assigned to AUSTRAC intelligence analysts to assess and respond in accordance with our national security and law enforcement intelligence priorities. Additionally, through direct online access to AUSTRAC's intelligence system, SMR information is available to over 6,000 users from more than 35 of AUSTRAC's partner agencies to inform their intelligence gathering efforts and investigations.

Guidance on submitting SMRs can be found on [AUSTRAC's website](#).

# CRIMINAL THREAT ENVIRONMENT



AUSTRAC assesses the criminal threat facing Australia’s superannuation sector as **medium**.

The criminal threat environment refers to the nature and extent of ML/TF and other predicate offences associated with the sector.

The sector continues to be exposed to a similar variety of threats identified in the 2016 assessment, ranging from low-level individual and opportunistic offending through to large-scale attacks perpetrated by organised crime syndicates. Money laundering and predicate offences have highly likely evolved and increased in sophistication, particularly when cyber-enabled.

The primary threats facing the superannuation sector are attempts to claim illegal ERS payments and identity fraud, followed by scams, tax evasion and money laundering. The overall terrorism financing threat to the sector has likely declined in recent years.

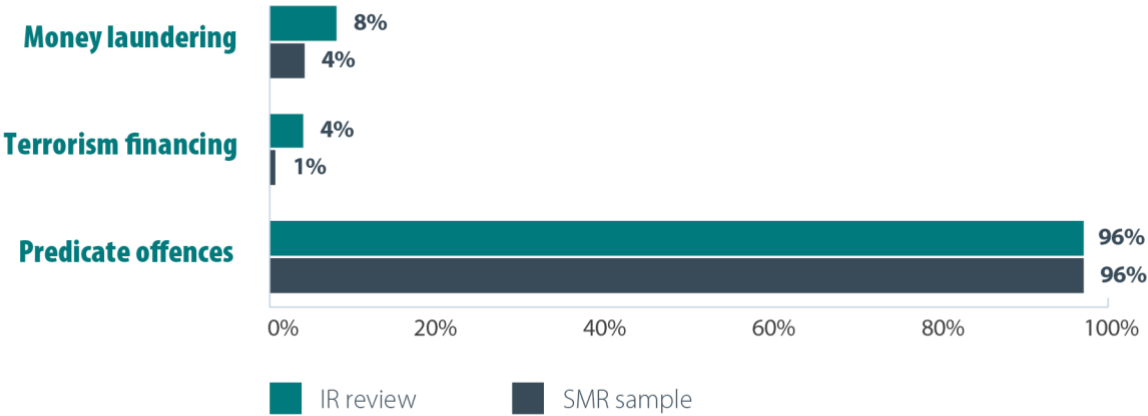


Figure 2: IR review and SMR sample comparison<sup>11</sup>

<sup>11</sup> Percentage amounts sum to more than 100 because some SMRs and IRs described more than one threat type.

## MONEY LAUNDERING

AUSTRAC assesses the nature and extent of money laundering threats facing the superannuation sector as **medium**. The extent of activity has highly likely remained consistent with the 2016 assessment, however AUSTRAC assesses the methodologies used to facilitate movement of funds have increased in complexity.

The superannuation sector is primarily exposed to money laundering at the placement and layering stages of the cycle as proceeds of crime can be disguised as superannuation funds when deposited, rolled over or withdrawn from a member's account. Amounts moving within or through the superannuation sector following a predicate offence – such as a perpetrator conducting an unauthorised rollover out of a victim's account using stolen personal identifiable information (PII) – are considered proceeds of crime. There is often a direct link between the predicate offences generating the proceeds of crime and the subsequent placement and layering activity, as proceeds generally remain in the superannuation system and are transferred between other superannuation accounts or SMSFs, until ultimately withdrawn. Figure 3 illustrates an example of how the superannuation sector is exposed to the money laundering cycle, where:

- **Placement** occurs when funds are moved out of a genuine superannuation account and are placed, now as the proceeds of crime, into another superannuation account.
- **Layering** occurs when the proceeds of crime continue to be moved through the superannuation system, via rollovers into other superannuation accounts or SMSFs, and ultimately withdrawn with the appearance of being a legitimate superannuation withdrawal.

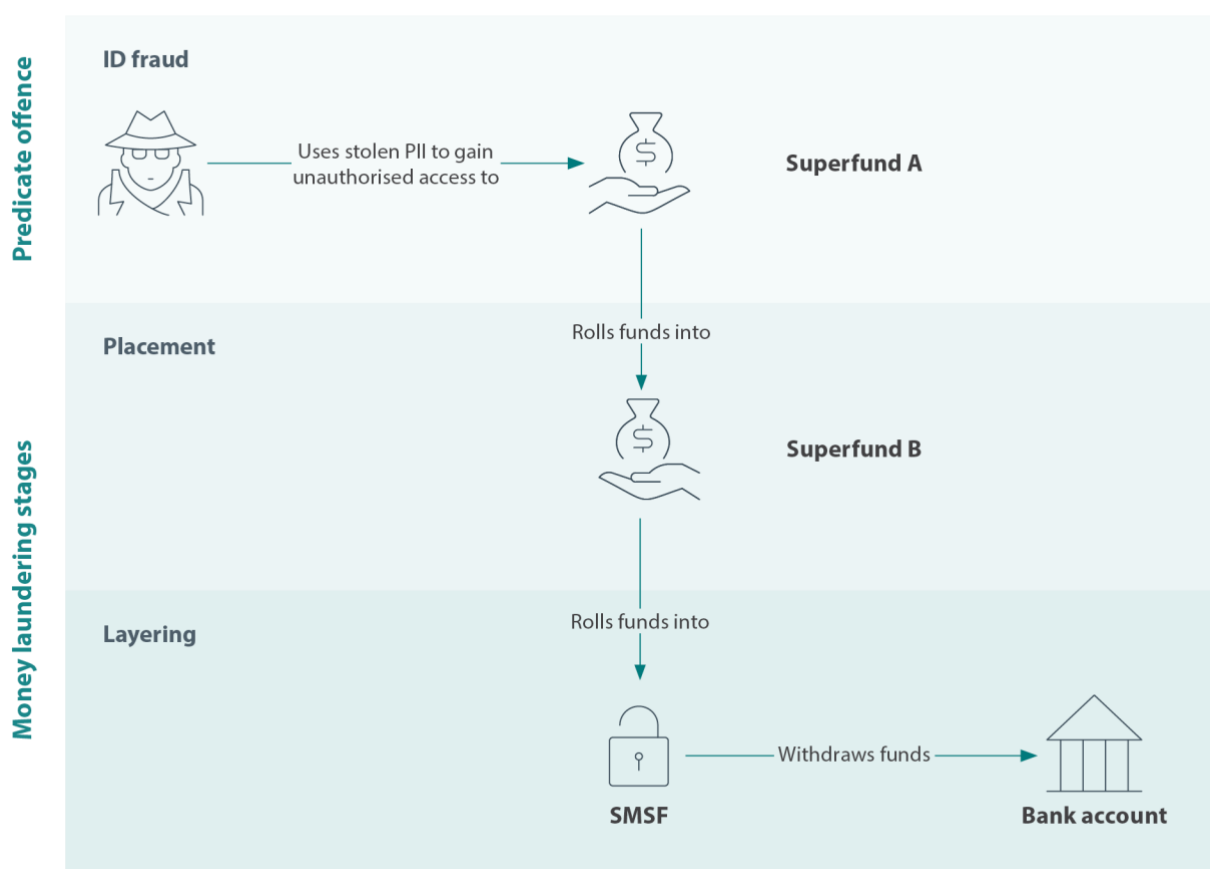


Figure 3: example of how the superannuation sector is exposed to the money laundering cycle

In the reporting period, suspected money laundering activity was identified in four per cent of the SMR sample and eight per cent of the IR review. The reported activity was characterised by:

- **structuring** – where a member is under the assumption that threshold transaction obligations apply to superannuation transactions, and makes a series of structured contributions or withdrawals under \$10,000 in an attempt to avoid detection.<sup>12</sup>
- **rapid or complex transfer of funds** – where a member makes unusually large and/or regular contributions, or conducts rollovers, followed by:
  - rapid transfers of funds between member accounts,
  - rollovers of funds into a separate superannuation fund or SMSF, or
  - benefit withdrawal requests.
- **unexplained wealth** – where a member makes unusually large and/or regular contributions that do not match their financial profile.
- **staging accounts** – where a member establishes an account for the purpose of consolidating or transiting through funds before they are further transferred or withdrawn from the superannuation system.

### Staging accounts

New superannuation accounts can be created as staging accounts and exploited by criminals to layer the proceeds of crime. These accounts can be used to receive rapid or unauthorised rollovers from other superannuation funds, or used to establish and provide credibility to false or stolen identities. Partner agencies described criminals creating accounts to test the useability of stolen PII, to identify vulnerability points within the superannuation system, and to determine whether funds could flow through the various mechanisms of the system, and ultimately be withdrawn.

Under the AML/CTF Act know your customer (KYC) procedures may only occur at points of outgoing activity, which does not include rollover activity. This enables new accounts to be created and used without undergoing identification checks. Advances in technology, such as the digitisation of systems, has also increased the ease and speed of creating new accounts.

The SMR review identified common indicators for the creation of staging accounts, including member accounts set up using:

- common email addresses, residential addresses, or phone numbers,
- closed or invalid email addresses,
- disposable email addresses, which are active for a specified period of time. For example, one provider of disposable email addresses limits usage to 60 minutes before the email is discarded, or
- stolen PII.

<sup>12</sup> AUSTRAC acknowledges that some early release benefits are limited to \$10,000. However, this reported activity is reflective of specifically observed structuring behaviour.

### CASE STUDY: SUSPICIOUS ROLLOVERS THROUGH STAGING ACCOUNTS

One fund identified a scheme where rollovers and severe financial hardships claims were used as a vehicle to move potentially illegal funds through superannuation accounts and funds.

Staging accounts were created as a layering mechanism to receive and disperse money obtained fraudulently, where fourteen individuals joined the fund via online channels and shared a common email. When joining the fund, all individuals advised they were unemployed and used similar user names for their online accounts.

The individuals conducted multiple transfers—totalling just under \$10,000 per transaction—in and out of the fund, highly likely layering the transactions across multiple superannuation funds. Each member also submitted a financial hardship claim. The similarities may indicate the accounts were controlled by another entity.

A search for the common email address in AUSTRAC holdings revealed numerous SMRs had been submitted by various superannuation funds, indicating the scheme was laundering the proceeds of illegal ERS across multiple funds. These SMRs detail suspicious rollovers, indicating the intent to possibly avoid the threshold of \$10,000, and the submission of multiple financial hardship claims within a 12 month period. It was observed the financial hardship documents contained the same handwriting and the certified documents were all witnessed by the same person.

### Self-managed superannuation funds

SMSFs are being used by criminals to facilitate financial crime against the superannuation sector, and used as a vehicle to move funds through and out of the system. Over 61 per cent of questionnaire respondents listed instances of fraud involving SMSFs, with rollovers commonly routed to SMSFs, either by members perpetrating illegal ERS, or by criminals defrauding funds, and then withdrawing them from the SMSF bank account. It is likely criminals use this approach as it is easier to withdraw funds through this avenue, as SMSFs are controlled and operated by the SMSF members themselves or a trusted advisor, in comparison to the arm's length nature of APRA-regulated funds.

The speed of this activity has been accelerated by legislative changes, requiring that rollovers to SMSFs be completed within three business days. This poses challenges for reporting entities trying to mitigate risk associated with this activity. SMSFs also afford criminals the opportunity to steal the entire balance by withdrawing it from the SMSF bank account, as opposed to other common fraud types (typically ERS) where only a small portion of the balance is available.



## TERRORISM FINANCING

AUSTRAC assesses the extent and nature of terrorism financing threats facing the superannuation sector as **low**. This is based on the low number of terrorism financing-related SMRs submitted by the sector in the SMR sample, findings from the IR review and information obtained during consultations.

The extent of the current threat posed by known and suspected terrorism financing in the sector has decreased since the 2016 assessment. In the reporting period, one per cent of the SMR sample and four per cent of the IR review related to suspected terrorism financing. Suspicious activity or indicators included:

- members identified on a watch list, law enforcement action or open source information relating to terrorism financing
- member details matching those of an individual previously convicted of involvement in terrorist activity or financing in a foreign jurisdiction
- a member linked to terrorism financing opens an account, makes contributions and then submits a claim for that amount within a short period of time
- members with possible name matches to a known terrorist, attempting to claim a superannuation death benefit with fraudulent identification documentations.

Superannuation funds are required to accept new members, regardless of their ML/TF risks. AUSTRAC acknowledges that this requirement can present certain challenges, and encourages reporting entities to have robust processes detailed in their AML/CTF program to manage the risks associated with these members, including heightened and regular transaction monitoring, and further SMR reporting as appropriate. Reporting entities should remain vigilant to shifts in the domestic and global terrorism environments and their impact on terrorism financing activity.

### AUSTRALIA'S TERRORISM FINANCING ENVIRONMENT

Since the territorial collapse of Islamic State of Iraq and the Levant's caliphate in Syria and Iraq, there has been a sharp decline in the number of foreign terrorist fighters departing Australia. However, the security environment continues to evolve and the emergence of the COVID-19 pandemic, while inhibiting some aspects of the terrorism threat through the restricted cross-border movement of people, has also presented a platform for recruitment and the promotion of extremist narratives online. Amid this evolving environment, supporters and sympathisers in Australia are likely to continue to send funds internationally in support of terrorist activity.

The primary threat to Australia stems from religiously motivated violent extremism in the form of lone actors or small groups, although ideologically motivated violent extremism poses an increasing threat. These actors and groups primarily conduct small-scale, low-cost terrorist attacks using weapons that are inexpensive and easy to acquire, and tactics that do not require specialist skills. The national terrorism threat level at the time of publication is assessed by the National Threat Assessment Centre as **probable**.

It is unlikely significant amounts of terrorist-related funds are flowing into, through or returning to Australia from offshore. Financial outflows may increase if returned foreign fighters begin sending funds to regional countries or radicalise vulnerable members of the community. Restrictions on cross-border movements imposed in response to the COVID-19 pandemic are likely to have limited the ability for foreign fighters to return to Australia. These restrictions also likely affected the ability for cash to be moved into or out of Australia for terrorism financing purposes.

## PREDICATE OFFENCES

AUSTRAC assesses the nature and extent of threat posed by predicate offending involving the superannuation sector as **high**. This remains largely consistent with the 2016 assessment, however the sophistication in methodologies and extent of offences has increased and evolved.

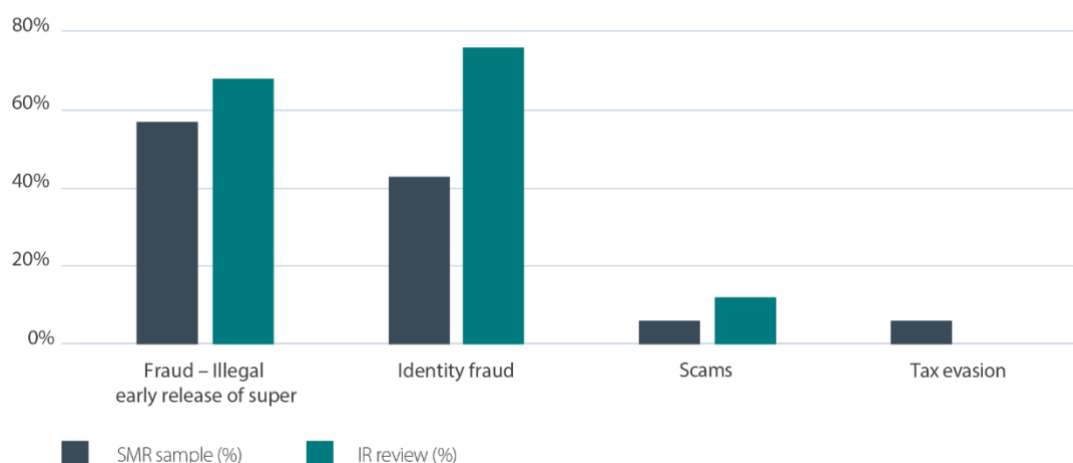


Figure 4: Predicate offences identified in the SMR sample and IR review

## CYBER-ENABLED SUPERANNUATION FRAUD

Cybercrime continues to be an enabler of superannuation fraud, and is often associated with predicate offending in the sector. Twenty-one per cent of the SMR sample described cyber-enabled suspicious activity, and of this, 73 per cent involved identity fraud and 46 per cent involved illegal ERS.

Fraud facilitated by cybercrime has increased in sophistication since the publication of the 2016 assessment, which emphasised organised crime groups stealing a sole individual's PII, indicating the scale of the attacks were smaller. However, criminal activity in the current reporting period ranges from low-level individual and opportunistic offending through to large-scale attacks perpetrated by organised crime syndicates. This includes targeting PII data through attacks on superannuation funds, employer payroll systems, and third-party businesses or entities, such as tax agents, who hold a large pool of member identity and superannuation data.

Cybercrime can occur through various means. This includes the exploitation of the sector's digitisation of services that are reliant on online platforms (see 'Illegal early release of super' on page 19), new superannuation accounts established offshore using compromised PII (see 'Identity fraud' on page 20), and the use of phishing campaigns, hacking and/or cyber-intrusion activities (see 'Scams' on page 21). Alternatively, perpetrators of superannuation fraud can purchase compromised PII in bulk from cyber-criminals on the darknet (see 'Data as a commodity' on page 24).

## Fraud – Illegal early release of super

Attempts to gain illegal ERS<sup>13</sup> remains the most reported suspicious activity by the sector, identified in 57 per cent of the SMR sample and 68 per cent of the IR review. This activity was conducted by superfund members themselves, who attempt to gain access despite being ineligible, as well as third parties perpetrating superannuation fraud. Common themes included:

- claims through the Australian Government's temporary COVID-19 ERS program (see page 6 for further information) and other ERS programs
- rollovers of superannuation balances to SMSFs for the early withdrawal of funds
- rollovers of superannuation balances to various funds, followed by separate financial hardship claims at each fund to circumvent the maximum \$10,000 amount that can be released under this criteria
- perpetrators of fraud submitting ERS claims using stolen PII and/or falsified identity information.

### USING FALSIFIED DOCUMENTATION TO ACCESS PAYMENTS

Some claimants also provided funds with falsified documents to support attempts to gain early access to superannuation or claim fraudulent insurance payments. Suspicious activity or indicators include:

- falsified documents purportedly from Services Australia in support of a financial hardship claim
- falsified birth certificates in an attempt to gain illegal access to a pension fund
- falsified death certificates in an attempt to obtain a death benefit payment
- falsified medical certificates in an attempt to gain access to an insurance benefit paid out by the superannuation fund
- use of the same or unregistered Justice of the Peace to certify falsified documents for different members.

AUSTRAC assesses the sophistication of methodologies for illegal ERS attempts has remained consistent with those in the 2016 assessment, however the extent of such activity has increased.

Recent temporary early release schemes combined with continuing technological changes have made it easier for individuals to access superannuation services through online platforms. They also allow members to amend some account details, apply for withdrawals, or electronically certify documents without face-to-face contact with their super fund. Some funds indicated that while digitisation is convenient for members who are legitimately withdrawing funds, the ease of access has also increased the number of attempts by individuals seeking to gain illegal ERS payments. This includes exploitation by organised crime groups conducting large-scale attacks utilising bulk data, then using the stolen PII to claim illegal ERS payments.

One fund also observed an increase in the number of financial hardship claims from newly-joined members. Members can create new accounts at multiple funds for the purpose of illegally obtaining multiple ERS payments. Superannuation balances are rolled over between the various funds, and within a year, a member can submit many ERS claims. As this is not centrally regulated, it is highly likely criminals and opportunistic individual offenders manipulate this for financial gain.

<sup>13</sup> Superannuation can be released before preservation age in limited circumstances, including severe financial hardship, compassionate grounds, death benefit payments, total and permanent disablement, income protection and trauma payments.

## COVID-19

In March 2020, the Australian Government announced assistance to support individuals and businesses to manage the economic impact of the COVID-19 pandemic. Eligible individuals financially impacted by COVID-19 were able to apply online with the ATO through myGov to access up to \$10,000 of their superannuation during the 2019-20 financial year and up to \$10,000 between 1 July 2020 and 31 December 2020.<sup>14 15</sup>

The volume of ERS claims increased during the above period and included unlawful exploitation by individuals who were ineligible, as well as organised crime groups using the temporary ERS scheme as an opportunity to gain access to funds using stolen PII already in their possession. During this period, funds were exempt from conducting customer verification for payments approved by the ATO when related to the COVID-19 ERS scheme.<sup>16</sup> This enabled flexibility in an existing legislative control, likely contributing to the increased attempts to fraudulently access superannuation payments.

During the reporting period, the majority of illegal ERS activity (69 per cent of illegal ERS-related SMRs and 87 per cent of illegal ERS-related IRs) involved attempts to withdraw funds through the COVID-19 ERS scheme. In addition, one partner agency found that 76 per cent of superannuation frauds reported to their organisation between April 2020 and January 2021 were also related to COVID-19 ERS.

A small number of SMRs (eight per cent of illegal ERS-related SMRs) also identified suspicious behaviour indicative of taking advantage of the COVID-19 ERS scheme for tax avoidance purposes. These members withdrew funds under the scheme and then, within a short timeframe, redeposited the funds to their account.

## Identity fraud

AUSTRAC assesses the nature and extent of identity fraud has increased since the 2016 assessment, and is present in 43 per cent of the SMR sample and 76 per cent of the IR review. This is due to a growth in opportunities for offenders to obtain compromised PII, such as PII purchased from cyber-criminals on the darknet or obtained through low-level frauds conducted by offenders known to a member. For example, an ex-spouse or relative using PII documents to access the member's superannuation account without authorisation. Intelligence also indicates increased involvement by organised crime groups who are targeting businesses or entities to obtain PII for a large pool of members, as opposed to targeting individuals. Access to the high number of PII can create increased opportunities for criminals to conduct superannuation fraud.



Another form of identity fraud involves the use of falsified identity documentation to support superannuation fraud. This can include documents that have been altered and used to conduct unauthorised transactions on a member's account (see page 19 for indicators of this activity).

<sup>14</sup> Individuals could apply for COVID-19 temporary ERS payments between 20 April 2020 and 31 December 2020. Eligible temporary residents were able to access up to \$10,000 of their superannuation in 2019–20 only.

<sup>15</sup> ATO, *COVID-19 Early release of super report*, [https://www.ato.gov.au/uploadedFiles/Content/SPR/downloads/covid19\\_early\\_release\\_of\\_super\\_report\\_infographic.pdf](https://www.ato.gov.au/uploadedFiles/Content/SPR/downloads/covid19_early_release_of_super_report_infographic.pdf).

<sup>16</sup> AUSTRAC, *New customer verification AML/CTF Rule to support early release of superannuation initiative*, <https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/new-customer-verification-amlctf-rule-support-early-release-superannuation-initiative>.

Compromised PII can be used to conduct account takeovers, where the offender fraudulently accesses a member's superannuation account to:

- conduct withdrawals,
- submit illegal ERS claims if the member has not reached preservation age,
- authorise rollovers out of the member's account into an account controlled by the offender, and ultimately withdrawn. This may include rollovers between several superannuation funds to obscure funds flows, or
- update the personal details of the member, such as replacing contact information with the offender's contact details and/or new bank account information.

In addition, compromised PII can be used to establish new superannuation accounts, including staging accounts, or SMSFs, to receive stolen funds and act as an additional mechanism to obscure funds flows.

### CASE STUDY: FRAUDULENT ACCOUNT OPENINGS FROM AN OVERSEAS JURISDICTION

A superannuation fund identified 155 suspicious accounts which were opened online, all within a three week period and likely using fraudulent IDs. The personal details used to establish the new accounts had similar discrepancies, such as identical mobile numbers, email addresses, and incomplete or incorrect residential addresses. Additionally, the IP addresses used to open all 155 accounts were traced to the Philippines.

The ATO's SuperMatch<sup>17</sup> service was used when the accounts were opened, which successfully returned results of each member's superannuation balance based on ATO records. This suggests the name, date of birth and tax file number details supplied for each account were correctly provided and likely obtained fraudulently. No transaction activity was present in any of the new accounts, however the perpetrators were likely attempting to obtain superannuation information through SuperMatch to facilitate future fraudulent activity.

The fund attempted to contact the members using the mobile phone numbers provided however was unsuccessful, as the numbers appeared to be invalid, further indicating potential identity fraud and cybercrime activities.

## Scams

AUSTRAC assesses the complexity of scams has increased since the publication of the 2016 assessment. Intelligence holdings and consultations detail the length and sophistication employed by criminals to impersonate a third party to illegally obtain superannuation funds. It is likely the increased sophistication is also due to the shift from paper forms to online platforms, with 77 per cent of industry respondents identifying instances of scams involving financial advisers, false investments schemes, websites, and online access to member accounts.

Scams were identified in six per cent of the SMR sample and 12 per cent of the IR review. Common themes included:

- Criminals using phishing techniques or establishing fraudulent websites to create legitimacy for their scams.

<sup>17</sup> The SuperMatch service gives superannuation fund trustees access to details of active super fund accounts, including lost or ATO-held accounts. This helps super fund trustees with the consolidation of super accounts for their members. ATO, *SuperMatch*, <https://www.ato.gov.au/super/superstream/in-detail/validation-services/supermatch/>.

- Criminals portraying themselves as financial advisers or brokers, contacting members and often employing cold-calling techniques to lure victims. When successful, members voluntarily provide PII and/or identity documents to criminals.
- The use of investment scams, such as cryptocurrency scams, enticing members to transfer their superannuation balances for investment purposes.
- Criminals targeting employer data, and then conducting business email compromise and remote access scams to gain access to employee superannuation accounts.
- SMSF accounts used as staging accounts, set up for the sole purpose of receiving unauthorised or illegal benefits/balance(s).

One fund noted that since the publication of the 2016 assessment, there has been an increase in scams involving criminal actors posing as independent financial advisers and financial counsellors. Offenders advertise and use aggressive cold calling tactics, convincing members to withdraw their superannuation and invest into false investment schemes, or target vulnerable members to access their superannuation funds under false hardship claims. By gaining authority to act on behalf of the member, the financial advisor can submit certified identification and withdrawal requests. The financial advisor will retain a large percentage of the funds and transfer the remaining balance to the member's genuine bank account. An indicator of this activity is that there is minimal, if any, member engagement or contact.

In addition, AUSTRAC assesses the presence of SMSF scams is increasing, with fake advisor scams demonstrating a degree of complexity, patience and expertise. These also involve criminals establishing online profiles such as a financial advice or investment company, cold calling victims, and the perpetrator can take considerable time to establish a trusted relationship. The perpetrator then convinces the victim to establish an SMSF and authorise the fake advisor to act on their behalf. Funds are then transferred to the SMSF which is controlled by the criminal, and stolen. In one instance, a member used these services to establish an SMSF, which resulted in their entire superannuation benefit of over \$310,000 defrauded.



AUSTRAC acknowledges that fraud and scam criminal threats are continually evolving. Although some activity can be difficult for a reporting entity to identify, particularly where activity occurs outside of the superannuation sector, reporting entities should remain vigilant to the threats relevant to their operations and members.

AUSTRAC encourages the sector to:

- promote member education and awareness,
- continue strengthening fraud mitigation systems and controls, and
- report suspected fraud and scam-related activity in SMRs.

## Tax evasion

The superannuation sector does not appear to be a significant vehicle for tax evasion, with six per cent of the SMR sample relating to suspected tax evasion offences.<sup>18</sup> AUSTRAC assesses that although the extent of tax evasion-related activity remains consistent with the 2016 assessment, the nature of the methodologies used to facilitate this activity have changed. This is due to almost all SMRs describing individuals taking advantage of the recent COVID-19 ERS scheme. These members were reported for

<sup>18</sup> The IR review did not identify tax evasion-related offences.

receiving early release payments, followed by subsequent redeposits of the same amount into the fund in order to claim tax deductions as deductible personal superannuation contributions.

Observations from industry also identified possible tax evasion tactics, including:

- the diversion of income into super, where it is taxed at a concessional rate or can be treated as a tax exemption, or
- employers conducting voluntary contributions above the concessional cap for fake employees, followed by attempts to obtain refunds on the premise of erroneous contributions



## SIGNIFICANT SHIFTS

### Data as a commodity

In the 2016 assessment data security was identified as a critical vulnerability. This has increased due to the growth in connectivity of online platforms related to internal operations, systems and services. This has resulted in a shift which has seen cybercriminals targeting superannuation funds for their data alone. This is a significant change in offending behaviour from targeting member money, to targeting the data held by the Trustee.

The theft and on-selling of bulk PII is a lucrative crime. In 48 per cent of questionnaire responses, and supported by consultations, funds and industry have reported the risk posed by compromise of the significant amount of data held by funds. Once compromised, criminal entities may use the PII to conduct fraud, or sell the PII to fraud facilitators on the darknet. It is highly likely that criminals will often have enough credentials to compromise a member's superannuation account, defraud Commonwealth Government services and commit other financial crimes. AUSTRAC acknowledges this predicate offence of data theft is a separate activity to superannuation fraud.

Further, compromised PII may be one component of wider fraudulent activity occurring. It is likely that when a compromised superannuation account is identified it represents just one element of broader offending targeting a range of financial or government products. The below diagram (figure 5) illustrates how this occurs.

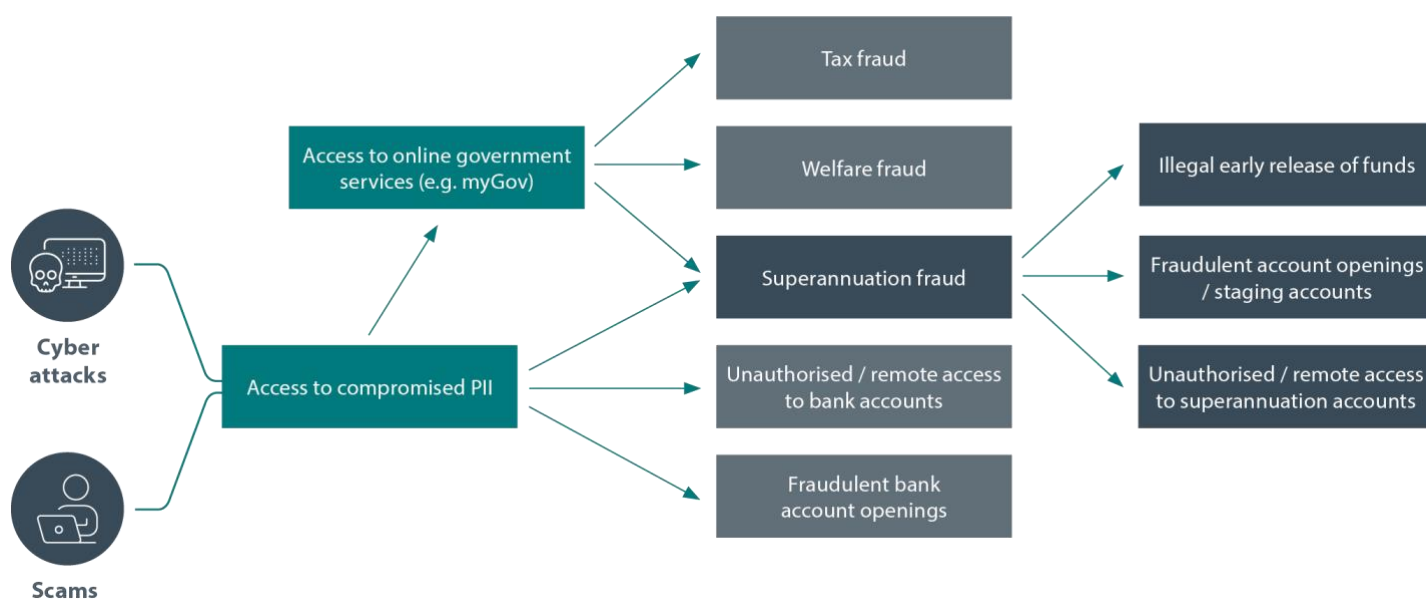


Figure 5: Demonstrates how the access to compromised PII can contribute to the exploitation of various financial services.

Criminals typically have agile illicit business models and are attracted to cybercrime because it provides speed, large volumes of data, and low operating costs. The actual extent of these activities is likely under-reported due to superannuation funds not always having visibility over the cyber-enabled aspect of a fraudulent account creation or transaction. Further, this activity can be difficult for reporting entities to identify because it occurs outside of the designated services of the sector. AUSTRAC acknowledges the challenges superannuation funds face in this area, and encourages the continued reporting of SMRs to identify any suspicious activity that arises. SMRs provide crucial pieces of intelligence that form part of a larger picture of offending.



## EMERGING RISKS

Emerging risks refers to threats or vulnerabilities that are new or have changed since the 2016 assessment.

AUSTRAC has identified several emerging risks facing the superannuation sector. The identified emerging risks are significant and are enabled by technological and legislative changes.

### Family fraud, elder abuse and domestic violence

Family fraud, elder abuse, and financial abuse associated with domestic violence describes activity where superannuation funds are fraudulently withdrawn by a family member, spouse, relative or housemate. Industry consultations highlighted this activity as a prevalent threat associated with early release schemes, particularly when claims can be submitted through online platforms without face-to-face interaction with the superannuation fund. This activity was also identified by almost half of the industry questionnaire respondents and characterised by:

- **financial abuse** – the victim may be subjected to financial abuse where they are forced to withdraw funds from their superannuation account.
- **fraud through identification theft/compromise** – PII can be compromised where member information and details are easily accessible and available to family members, partners or housemates, who may conduct unauthorised withdrawals and rollovers, or change the member's contact details to their own. This includes small withdrawals, including from pension accounts, which are harder to detect.
- **financial activity inconsistent with member profile** – the level of interaction and financial activity does not match the customer profile.

AUSTRAC is aware of increased instances of domestic violence during the COVID-19 pandemic and the implementation of lockdowns,<sup>19</sup> which may have contributed to the emergence of financial abuse in the superannuation sector associated with domestic violence. Further, AUSTRAC assesses the extent of this activity is likely under-represented in SMR reporting and intelligence holdings due to the challenges in detecting this activity and the unwillingness of victims to report financial abuse.

### CASE STUDY: SUSPECTED FAMILY FRAUD

A fund was contacted by a member to advise their recent COVID-19 release payment was not requested by them. The member believed this to be an instance of family fraud as the member's spouse had accessed their online accounts and requested the payment. The member was alerted to this activity after attempting to submit a COVID-19 early release request.

### Merger activity

Industry consultation identified the growing volume, scale and pace of merger activity across the sector as an area of concern. Successor funds may not be assessing the AML/CTF risk profiles of the bulk volume of members being ingested, or considering the strength of the incoming fund's AML/CTF program and how this impacts their own AML/CTF risk assessment of the combined fund.

In addition, the successor fund may lose, or have limited access to, the profile history of the new members. This impacts the fund's ability to understand the AML/CTF risk, as members' transaction

<sup>19</sup> Australian Financial Review, *Melbourne lockdown sends domestic violence 'through the roof'*, <https://www.afr.com/policy/health-and-education/lockdown-weaponises-domestic-violence-20200806-p55j2r>.

history may be reset as a result of the merger. Funds may not be aware of suspicious activity previously associated with the members, for example, a member's attempts to gain illegal ERS payments. Funds will benefit from robustly assessing the AML/CTF program and membership profile of the incoming fund, assessing the ML/TF risk of the merger and ensuring that controls and transaction monitoring remain fit for purpose during any merger process.

## Stapling

Several questionnaire respondents have raised concerns about stapling and the ML/TF risk to the superannuation sector. In most cases this was in relation to stapling's vulnerability to abuse by fake employers, opportunities to compromise member PII, or launder funds.

A stapled super fund is an existing super account that is linked, or 'stapled', to an individual employee so it follows them as they change jobs: employers may access information about employees' stapled fund through the ATO's online portal. Vulnerabilities that were noted included:

- the establishment of fake employers, or impersonation of legitimate employers, to access member superannuation details and PII through the stapling portal
- use of an established member account to launder funds – a member may not know the funds are moving through their account if it has been used by a new employer
- manipulation of the system to establish accounts, introduce and move funds for laundering purposes with no KYC requirements prior to exiting the sector
- increased opportunity to establish and operate an account using stolen PII due to decreased face-to-face touchpoints.

## APPENDIX A: GLOSSARY

NAME	DESCRIPTION
<b>AML/CTF</b>	Anti-money laundering and counter-terrorism financing.
<b>AML/CTF program</b>	A document that sets out how a reporting entity meets its AML/CTF compliance obligations.
<b>Darknet</b>	Part of the internet that is hidden from the view of typical search engines and only accessible by means of additional networking protocols and special software. It allows users and website operators to remain anonymous or untraceable.
<b>Early release of superannuation (ERS)</b>	Limited circumstances that allow superannuation to be released before preservation age and include financial hardship, compassionate grounds, death benefit payments, total and permanent disablement, income protection and trauma payments.
<b>Integration</b>	The final stage of the money laundering cycle, in which illicit funds or assets are invested in further criminal activity, 'legitimate' business or used to purchase assets or goods. At this stage, the funds are in the mainstream financial system and appear to be legitimate.
<b>Layering</b>	The second stage of the money laundering cycle, which involves moving, dispersing or disguising illegal funds or assets to conceal their true origin.
<b>ML/TF</b>	Money laundering and terrorism financing.
<b>Personally identifiable information (PII)</b>	Information that can be used to identify, contact or locate an individual.
<b>Phishing</b>	Phishing scams (either online or by phone) are attempts by scammers to trick individuals into giving out personal information such as bank account details, passwords and credit card numbers. <sup>20</sup>
<b>Placement</b>	The first stage of the money laundering cycle, in which illicit funds first enter the formal financial system.
<b>Predicate offence</b>	For the purpose of this assessment, a predicate offence is any offence which generates proceeds of crime.
<b>Preservation age</b>	Preservation age is the age you can access your super if you are retired (or start a transition to retirement income stream).
<b>Rapid or complex transfer of funds</b>	Transactional activity which does not appear to make financial sense.
<b>Remote access scams</b>	Remote access scams (also known as technical support scams) usually involve scammers contacting people over the phone to get access to their computers in an effort to steal their money.
<b>Rollover</b>	A rollover is when a member transfers some or all their existing super between funds.

<sup>20</sup> <https://www.scamwatch.gov.au/types-of-scams/attempts-to-gain-your-personal-information/phishing>

<b>Self-managed super fund (SMSF)</b>	An ATO-regulated superannuation fund that meets the requirements in section 17A of the Superannuation Industry (Supervision) Act 1993. These are limited to six or less members. All are either trustee directors, or directors of the corporate trustee of the fund.
<b>SOCG</b>	Serious and organised crime group.
<b>Staging accounts</b>	An account established for the purpose of consolidating funds before they are transferred.
<b>Stapling</b>	A stapled super fund is an existing super account linked, or 'stapled', to an individual employee so it follows them as they change jobs.
<b>Structuring</b>	Making or receiving a series of cash transactions intentionally structured to be below the \$10,000 reporting threshold.
<b>Suspicious matter report (SMR)</b>	A report a reporting entity must submit under the AML/CTF Act if they have reasonable grounds to suspect that a transaction may be related to money laundering, terrorism financing, tax evasion, proceeds of crime or any other serious crimes under Australian law. An SMR must also be submitted if the reporting entity has reasonable grounds to suspect the customer or an agent of the customer is not who they say they are.
<b>Transnational, serious and organised crime</b>	<p>Transnational, serious and organised crime covers a wide range of the most serious crime threats impacting Australia including:</p> <ul style="list-style-type: none"> <li>• manufacture and trade of illicit commodities, including drugs and firearms</li> <li>• sexual exploitation of children</li> <li>• human trafficking and slavery</li> <li>• serious financial crime</li> <li>• cyber crime.</li> </ul> <p>Key enablers of transnational, serious and organised crime include money laundering, identity crime and public sector corruption.</p>
<b>Unexplained wealth</b>	The source of the funds, or the source of an individual's wealth, is unclear or is inconsistent with their profile.

## APPENDIX B: METHODOLOGY

The methodology used for this report follows Financial Action Task Force guidance, which states that ML/TF risk at the national level should be assessed as a function of criminal threat, vulnerability and consequence.

This report considered six risk factors across the above three categories and each risk factor was assessed as 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. The average of the risk scores for each risk factor provides the overall criminal threat environment risk rating for the sector.

CRIMINAL THREAT ENVIRONMENT		
LOW	MEDIUM	HIGH
Minimal variety of money laundering methodologies. There is a low level of involvement by SOCGs and other higher-risk entities.	Money laundering methodologies are moderately varied. There is a medium level of involvement by SOCGs and other higher-risk entities.	Money laundering methodologies are highly varied. There is a high level of involvement by SOCGs and other higher-risk entities.
Low number of money laundering cases in the sector, and low associated values.	Moderate number of money laundering cases in the sector, and moderate associated values.	High number of money laundering cases in the sector, and high associated values.
Minimal variety of terrorist financing methodologies. None or a very small number of terrorist groups and their financiers, associates and facilitators utilising the sector.	Terrorist financing methodologies are somewhat varied. There is a small number of terrorist groups, financiers, associates and facilitators utilising the sector.	Terrorist financing methodologies are highly varied. There are several terrorist groups, financiers, associates and facilitators utilising the sector.
Very few instances of terrorism financing in the sector, with negligible or very low associated values.	Some instances of terrorism financing in the sector, with low associated values.	Multiple instances of terrorism financing in the sector, with moderate or high associated values.
Minimal variety of predicate offences. There is a low level of involvement by SOCGs and other higher-risk entities.	Predicate offences are moderately varied. There is a medium level of involvement by SOCG and other higher-risk entities.	Predicate offences are highly varied. There is a high level of involvement by SOCG and other higher-risk entities.
Low number of predicate offences in the sector, and low associated values.	Moderate number of predicate offences in the sector, and moderate associated values.	High number of predicate offences in the sector, and high associated values.



AUSTRAC.GOV.AU

