Superannuation fraud

Latest date of information: 15 July 2016

Key indicators for industry

The following is a list of possible indicators which may help industry to identify superannuation fraud and potential money laundering. The existence of a single indicator does not necessarily indicate criminal activity. In most cases, it is the existence of multiple indicators which raises suspicion of potential criminal activity. These indicators should be used to assist in identifying where further monitoring and reporting to AUSTRAC is required.

1. Contributions by a post-preservation age member shortly followed by withdrawals, particularly when this pattern is repeated over a period of time.

2. Member making large and/or regular contributions that appear inconsistent with occupation, age, employment status, income, or transaction history.

3. Regular contributions or withdrawals by a post-preservation age member below the AUD10,000 reporting threshold indicating attempts to avoid detection.

4. Post-preservation age account showing multiple contributions made by a third party below the preservation age, especially for amounts below AUD10,000.

5. Member receiving unusually large regular contributions from an employer where these payments vary in amount and do not seem to relate to superannuation guarantee payments.

6. Member requesting a payment following a change of contact details to an overseas jurisdiction, e.g. listing an international phone number or address.

7. Member submitting a withdrawal request after changing contact details (email, mobile number and/or address) or account log-in/password via the fund website.

8. Member submitting a withdrawal request with supporting documents that appear falsified including copies of a drivers licence, passport, bank statement or early release claim forms.

9. Member submitting multiple payment requests from an account in a short time period where payments are transferred into multiple accounts either of the same or different banks.

10. Member submitting a withdrawal request listing a third party bank account on a withdrawal request form.
11. Superannuation fund receiving a call from a caller unable to pass identity and security checks and provides an incorrect name, date of birth, address information or is unable to verify previous employment history. Caller may become irritated or terminate call abruptly during the security identification process.

12. Member failing to supply required identification information and refusing to respond to phone, email or mail contact in relation to a payment benefit claim.

13. Member submitting early release claim under financial hardship grounds shortly after an account balance rollover into a newly joined fund.

14. Several claims for early release under financial hardship by separate members of the same super fund, which appear to have been prepared by the same scheme promoter. Applications are made shortly after account balance rollovers into newly joined funds and show similar characteristics including:
   i) application forms that appear to be filled out using the same pen and handwriting, and contain the same reason for supporting the claim, e.g. to pay off outstanding debt;
   ii) documents showing evidence of outstanding debt containing the same account number and dollar amount of debt, where the name and address has been altered;
   iii) members providing the same contact email address; and
   iv) identification documents and statutory declarations certified by the same Justice of the Peace.

15. Member submitting Department of Human Services (DHS) approval letter for early release under compassionate grounds that appears inconsistent with standard letter template including font, format, gaps in the body of the letter, and reference number.

16. Member claiming early release of funds under financial hardship or compassionate grounds annually over a multiple year period.

17. Member claiming payout due to terminal illness using falsified medical documentation that contains forged doctor signatures and incorrect practitioner qualifications and contact details.

18. Partner or family member of allegedly deceased person using a death certificate showing inconsistencies with authentic template including: format of the listed date of birth and death; identity number; and date of birth on identification different from that on supplied death certificate.

Purpose

To inform AUSTRA’s industry partners about the methods associated with potential money laundering and fraud relating to superannuation funds. A list of indicators is provided to assist with the identification, monitoring and reporting of those persons engaged in this activity.

Background

The superannuation sector faces a number of threats from criminal entities. AUSTRA financial intelligence has identified three methods relating to the exploitation of superannuation funds from criminals likely attempting money laundering or to illegally gain access to superannuation payments using fraudulent means such as identity theft or falsified documentation.
This brief focuses on threats related to Australian Prudential Regulation Authority (APRA) regulated superannuation fund accounts regulated under the Superannuation Industry (Supervision) Act 1993 and is based on AUSTRAC analysis of suspicious matter reports (SMRs) submitted by our industry partners.

Money laundering methods

Method 1 – Money laundering through superannuation fund accounts

Superannuation fund accounts are susceptible to money laundering as they present criminals with a means to introduce the proceeds of crime into the financial system. SMRs submitted by industry partners highlight unusual deposits and/or withdrawals by members and employers that deviate from normal or usual patterns of transaction activity, including:

I. contributions by a post-preservation age member shortly followed by withdrawals, particularly when this pattern is repeated over a period of time;

II. large and/or regular contributions that appear inconsistent with member occupation, age, employment status, income or transaction history; or

III. regular contributions or withdrawals by a post-preservation age member below the AUD10,000 reporting threshold indicating attempts to avoid detection.

The sections and scenarios presented below highlight suspicious patterns of transaction activity related to superannuation funds that may be indicative of potential money laundering.

(a) Unusual contribution and withdrawal activity by post-preservation age member

Superannuation accounts of members that have met a condition of release\(^1\) are vulnerable to money laundering by the member and/or their associates. Unusual behaviour that departs from the normal use of the fund, such as the pattern of withdrawing funds shortly after contributions have been made, may be indicative of potential money laundering.

Scenario 1: Unusual superannuation contributions and withdrawals by post-preservation age member

Mr X is a member of a superannuation fund and has reached his preservation age. His employment history shows that Mr X’s employment end date occurred six years prior to joining his current fund. Despite his employment history Mr X’s superannuation fund account continues to show large superannuation guarantee contributions annually over a three year period. His account shows no activity for 11 months of the year and then intensive deposit and withdrawal activity in a one month period occurring just before the end of the financial year. The amounts deposited range from AUD12,750 to AUD35,000 with almost identical corresponding withdrawals. In this three year period, Mr X also attempts to deposit a bank cheque valued at AUD50,000 described as an employer contribution and personal contribution of AUD1,000.

Figure 1: Scenario 1: Unusual superannuation contributions and withdrawals by post-preservation age member\(^2\)

Superannuation accounts of retired members may also be used by third parties who are below the preservation age to launder illicit funds. Funds are deposited into the account of a retired member’s account by a third party. The third party gains access to the funds once they are withdrawn by the member.

---

1 A member can access their super when they have satisfied one of the conditions of release. These include: reaching the preservation age and retiring; reaching the preservation age and beginning a transition to retirement income stream while still employed; ceasing employment at or after the age of 60; or, are over 65 years old (even if not retired). When one of these conditions is met members can receive funds as either lump sum payments or as regular income payments and can continue to make contributions into their funds.

2 Scenarios are developed through the analysis of Suspicious Matter Reports (SMRs) and other financial intelligence. These SMRs have been referred to our partner agencies for further investigation.
The alternative to using their own superannuation account presents an advantage to third parties aged below the preservation age: they place potentially illicit funds into the system that accrue investment earnings and can subsequently access funds without having to apply for early release.

### Scenario 2: Third party use of a retired member’s super account

Mr X is a retired member. His son, Mr Y who is below the preservation age, has been making regular deposits into his father’s account over a five year period. The after-tax contributions made into Mr X’s account have been paid for by cheque and cash. All contributions over the five year period were below AUD10,000 and some are made on the same day or a few days apart. The deposited funds are subsequently withdrawn by Mr X and handed back to Mr Y.

**Figure 2: Scenario 2: Third party use of a retired member’s super account**

### (b) Unusual contributions by member below the preservation age

Superannuation funds offer a vehicle for long-term money laundering for those below the preservation age. The proceeds of crime can be placed into superannuation accounts as contributions, which accumulate investment earnings over the life of the fund. Eventually, legitimate money is received by way of a lump sum payment or as regular pension payments once the member becomes eligible.

Unusual contributions by a member below the preservation age can be characterised by being inconsistent with the member’s profile, for example a member making regular low-value or single high-value contributions that may appear inconsistent with their occupation, age, employment status, income or transaction history.

### (c) Unusual employer contributions

Superannuation fund accounts also present an opportunity to employers to potentially co-mingle and launder illicit proceeds. Business owners can legitimise illicit funds under the guise of employer contributions to complicit employees. Such contributions may appear unusual for genuine employer contributions, especially if the amounts are large, fluctuate widely or do not relate to superannuation guarantee payments.

**Scenario 3: Unusual superannuation fund contributions by an employer**

Mr Y, an employee of Company A, receives unusual employer contribution payments into his superannuation fund account over a three year period. The contributions over the period total approximately AUD82,600 but fluctuate widely on an annual basis indicating they are potentially not genuine employer contributions. A contribution of AUD40,000 was received in the first year followed by AUD16,000 in the second year. In the third year contributions of AUD1,000 and AUD25,600 are made on the same day. A year after Mr Y received his final superannuation instalment from his employer he withdraws the entire amount from his superannuation account and transfers it into a Self-Managed Superannuation Fund (SMSF).

**Figure 3: Scenario 3: Unusual superannuation fund contributions by an employer**

---

3 See previous footnote
4 See previous footnote
Method 2 - Identity theft

Identity theft is a method used to conduct superannuation fraud. A criminal will impersonate the actual member to gain access to their account and receive a payment/s. A legitimate member’s fund is accessed by obtaining personal information or documentation which is used to pass identification checks including name, date of birth, fund membership details, drivers licence, passport and bank and superannuation account statements.

Personal information may be obtained from stolen documentation, phishing\(^5\), or more sophisticated methods involving cybercrime whereby a criminal will hack into a member’s personal email account or into the systems of superannuation funds.

The following methodology outlines the way a criminal may impersonate an actual member to fraudulently gain superannuation payments:

1. A criminal will obtain enough personal information to impersonate the member.
2. In order to control all future correspondence with the fund the criminal changes the customer contact details, including address, phone number or email address by either:
   i) calling the fund and passing verifications checks;
   ii) submitting a change of contact details form with supporting falsified documentation; or
   iii) emailing the fund from the actual member’s personal email account.
3. The criminal then attempts to access a payment by either:
   i) submitting a withdrawal request form with supporting falsified documentation;
   or
   ii) making an online payment request.

Post-preservation age accounts are more susceptible to identity theft since there is no requirement to apply for early release.\(^6\) Cybercrime activity, such as hacking into personal email accounts, also enables criminals to fraudulently access a superannuation account from overseas jurisdictions as highlighted in Scenario 4.\(^7\)

<table>
<thead>
<tr>
<th>Scenario 4: Fraudulently accessing a post-preservation account</th>
</tr>
</thead>
<tbody>
<tr>
<td>An overseas-based organised crime group hacked into a post-preservation age member’s home computer and accessed personal information and monitored transactions from the 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. The crime group also diverted the member’s Australian phone number to an overseas number while they were overseas. 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.</td>
</tr>
<tr>
<td>In order to verify the payment the fund’s call centre staff called the diverted number and spoke to the fraudster who sounded like they were of the same demographic as the member. After passing 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.</td>
</tr>
</tbody>
</table>

\(^5\) Phishing is a scam by which criminals use the internet or short message service (SMS) to fraudulently obtain sensitive data from victims (for example usernames and passwords for online banking or superannuation accounts) by posing as a trustworthy source (for example, banks or government departments).  
\(^6\) Early release of super is explored in more detail in the following section: Method 3 – Illegal early release.  
\(^7\) This scenario is based on information provided during engagement with superannuation funds in preparing ASTRAC’s publication Australia’s superannuation sector: money laundering and terrorism financing risk assessment.
The one off lump sum payment was subsequently made to the member’s bank account. After noticing unusual transactions and changes to their bank account the member alerted their superannuation fund. The payment was subsequently frozen and not sent to the intended overseas destination.

**Figure 4:** Scenario 4: Fraudulently accessing a post-preservation account

Criminals fraudulently accessing payments by impersonating actual members are not limited to post-preservation age accounts. If the member is below the preservation age a criminal may attempt to submit an early release claim, for example on compassionate grounds, to access funds.

Scenario 5 highlights a criminal accessing two accounts from the same superannuation fund provider. The same Internet Protocol (IP) address was used to access multiple accounts where one account holder was below the preservation age.

**Scenario 5: Fraudulently accessing multiple superannuation fund accounts**

Mr X, a criminal, gains access to identity documents of two members of the same fund, members A and B. Member A is below the preservation age and member B above the preservation age. Mr X emails the fund purporting to be member A. He submits a change of details form and supporting documentation including a copy of member A’s drivers’ licence. As a result, the contact details on member A’s account are changed including a new email address and mobile number. Mr X then requests and receives a password via email. He then submits a withdrawal request based on compassionate grounds and provides a copy of a forged DHS letter. Days later a benefit payment is transferred into the criminal’s bank account.

In the same month, Mr X calls the fund purporting to be member B and after passing identification checks using the member’s name, date of birth and two additional pieces of personal information, changes the contact email address and adds a new mobile number. Mr X calls back and receives a password. Mr X proceeds to make 3 withdrawal requests over a two month period and provides a certified copy of member B’s drivers licence and a bank statement. Mr X receives his fraudulent payments in two bank accounts with the same bank.

**Figure 5:** Scenario 5: Fraudulently accessing multiple superannuation fund accounts

**Method 3 – Illegal early release**

There are limited circumstances under which a member may gain access to their super funds before reaching their preservation age. These include: severe financial hardship, compassionate grounds, terminal illness, permanent incapacity, and permanent departure from Australia. SMRs submitted by industry partners highlight the use of falsified or altered documentation by members to fraudulently gain early access to their superannuation. The use of fraudulent documentation to obtain early payments, which is relatively easy to attempt, presents a risk as the funds may possibly be used to support further illicit activities including terrorism financing.

(a) **Financial hardship claims**

Claims under financial hardship allow a member to obtain the maximum permissible amount of AUD10,000 over a twelve month period provided they have received government income support payments continuously for twenty-six weeks and are unable to meet reasonable and immediate living expenses.

Funds have observed members circumventing the AUD10,000 limit by submitting multiple claims. After receiving the maximum amount under financial hardship grounds from one fund, a member will...

---

8 Scenarios are developed through the analysis of Suspicious Matter Reports (SMRs) and other financial intelligence. These SMRs have been referred to our partner agencies for further investigation.


roll over their remaining balance into a new fund and then submit another claim for early release under financial hardship grounds within a short period of time (e.g. three months) of joining.

Many claims have involved the use of similar or identical documents by multiple members of the same fund. This seemingly coordinated approach may indicate the involvement of a scheme promoter or a criminal syndicate. These applications will show similar characteristics which include:

I. application forms that appear to be filled out using the same pen and handwriting and contain the same reason for supporting the claim, e.g. to pay off outstanding debt;

II. documents showing evidence of outstanding debt containing the same account number and dollar amount of debt, where the name and address has been altered;

III. members providing the same contact email address; and

IV. identification documents and statutory declarations certified by the same Justice of the Peace.

(b) Compassionate grounds and other early release claims

Applications under compassionate grounds are also vulnerable to exploitation by members using falsified or altered documentation particularly since the amount which can be potentially obtained, unlike financial hardship claims, is not capped. Early release claims under compassionate grounds require applicants to submit a Department of Human Services (DHS) approval letter to their superannuation fund.

In lodging fraudulent claims a member will provide a falsified or altered DHS approval letter indicated by inconsistencies with the authentic letter template including font, format, gaps in the body of the letter, and reference number. Some members alter previously used authentic approval letters to support multiple claims which show the same amount claimed for which the member previously applied.

Other examples of claims based on fraudulent documentation relate to terminal illness or death. A member feigns a terminal illness and provides falsified documents to support their claim containing forged doctor signatures and incorrect practitioner qualifications and contact details. Funds have also reported the use of falsified death certificates by a family member of the alleged deceased to fraudulently access death benefit payments.

Suspicious matter reporting

Reporting entities, should submit suspicious matter reports (SMRs) to AUSTRAC detailing any financial activity which they consider to be suspicious.

AUSTRAC assesses and disseminates relevant SMRs to law enforcement agencies and other authorities for their consideration. AUSTRAC also assists reporting entities to detect and deter money laundering by increasing their understanding of the vulnerabilities within their industry. By strengthening internal AML/CTF controls and programs, reporting entities can better undertake enhanced and ongoing customer due diligence, and develop policies and strategies to protect their services from being misused by criminals.

Questions and feedback

Please contact the AUSTRAC Contact Centre:

- Telephone: 1300 021 037

---

11 Although there is no set limit, the amount that can be withdrawn under compassionate grounds is limited to what is reasonably needed.
Email: contact@austrac.gov.au

Information is also available on the AUSTRAC website at www.austrac.gov.au
# Handling Instructions

**Limited distribution**

Reporting entities may use Methodologies Briefs (the material) internally, but only on a ‘need to know’ basis. Except for internal use, the material may not otherwise be used, copied, reproduced, published, altered or transmitted in any form or by any means outside the reporting entity in whole or part (except where such use constitutes fair dealing under the Copyright Act 1968 (Cth)) without the prior written approval of AUSTRAC.

The material is provided for general information only, and on the understanding that the Australian Government is not providing professional advice on a particular matter.

The material may include the views or recommendations of third parties, and does not necessarily reflect the views of the Australian Government, or indicate a commitment to a particular course of action.

The material may contain information that is intended to simplify legislation for ease of comprehension. In addition, errors or omissions can occur in the preparation of the material. The material is current at the time of publishing and is subject to change without notice to the user. Before relying on the material, users should independently verify its accuracy, completeness and relevance for their purposes and that it is up-to-date and/or obtain appropriate independent professional advice.

Links to other web sites are provided for the user’s convenience and do not constitute endorsement of material at those sites, or any associated organisation, product or service.