



**Phone** 02 9577 3333  
**Email** enquiries@superconsumers.com.au  
**Website** www.superconsumers.com.au  
57 Carrington Road,  
Marrickville NSW 2204  
**ACN** 163 636 566 | **ABN** 34 163 636 566

1 February 2024

Scams Taskforce  
Market Conduct and Digital Division  
The Treasury  
scampolicy@treasury.gov.au

### **RE: Scams – Mandatory Industry Code consultation**

Australians' retirement savings are at risk until all superannuation funds are required to prevent, detect, disrupt, and report super scams. When we refer to super scams, we refer to schemes designed to trick members into transferring their superannuation to a malicious third party, for example, a crypto scam targeting SMSF-holders, or a scammer posing as a financial advisor or investment firm.

Scams are a growing and urgent policy problem in Australia. While quantitative evidence on the prevalence of super scams is limited, in 2023 7,700 investment scams were reported to Scamwatch with Australians losing a total of \$276 million dollars.<sup>1</sup>

There are different forms of scams circulating the \$3.5 trillion super system. Common scams include:

- Self-managed super fund (SMSF) scams, where a scammer facilitates a member to create a self-managed super fund. The member's super is then transferred into a bank account controlled by the scammer, or the member is convinced to transfer some or all of their SMSF balance to the scammer.
- Post-preservation investment scams, where a member past preservation age is convinced to withdraw some or all of their funds and transfer them to the scammer.
- Early access scams, where a scammer encourages a member to fraudulently access their super under extreme financial hardship or compassionate grounds, and then the scammer takes a cut, or steals the funds or the member's identity.

Recent known super scams demonstrate the risk and depth of consumer harm, for example:

- An SMSF scam stole \$520,000 from six investors between 2015 and 2020,<sup>2</sup>

---

<sup>1</sup> Scamwatch, *2023 data*, <https://www.scamwatch.gov.au/research-and-resources/scam-statistics>

<sup>2</sup> ASIC 2023, *Former director sentenced to 4 years and 4 months imprisonment*, <https://asic.gov.au/about-asic/news-centre/find-a-media-release/2023-releases/23-349mr-former-director-sentenced-to-4-years-and-4-months-imprisonment/>

- An alleged \$1.3 million property investment scam pressured 14 people to withdraw from their super between 2016 and 2017,<sup>3</sup>
- Scammers operating out of a Manila call centre posing as a financial advice firm reportedly stole \$3.3 million in super from six people, discovered in 2022,<sup>4</sup>
- A couple lost \$220,000 in super after seeing a scam social media ad for an online trading platform in 2023,<sup>5</sup>
- A scammer posing as a financial advisor stole over \$23 million in super and savings from 72 people, uncovered in 2020.<sup>6</sup>

These are just some known, recent examples of super scams.

Since 2022, up to 178,000 superannuation members have been placed at heightened risk of phishing scams due to known super fund data breaches.<sup>7 8 9</sup> Data breaches can lead to an increased risk of phishing scams because scammers can use stolen personal information to target those who have been affected by the breach.<sup>10</sup>

These figures likely underestimate the total impact of super scams. The stigma associated with being scammed means there is a tendency for victims to underreport. Many people are less engaged with their super compared to other products and services, meaning they may not notice they have been a victim of a scam. Super Consumers consumer research suggests a fifth of people with super don't keep an eye on how much they have in their account, or read the communications their super fund sends them.<sup>11</sup> This means people may be less equipped to safeguard their savings compared to sectors where they are more engaged, like banking.

---

<sup>3</sup> ASIC 2023, *Gold Coast property developer charged with fraud*, <https://asic.gov.au/about-asic/news-centre/find-a-media-release/2023-releases/23-148mr-gold-coast-property-developer-charged-with-fraud/>

<sup>4</sup> ABC 2022, *Foreign call centre raided over alleged links to scam tricking Australians out of their superannuation*, <https://www.abc.net.au/news/2022-10-03/foreign-call-centre-raided-over-alleged-links-to-super-scam/101481678>

<sup>5</sup> Yahoo Finance 2023, *Sophisticated scam robs Aussie couple of entire \$220,000 superannuation savings*, <https://au.finance.yahoo.com/news/sophisticated-scam-robs-aussie-couple-of-entire-220000-superannuation-savings-212922925.html>

<sup>6</sup> ABC 2022, *Missing fraudster Melissa Caddick's luxury cars sold at auction for more than \$300,000*, <https://www.abc.net.au/news/2022-02-22/melissa-caddick-cars-sold-to-pay-back-fraud-victims/100850322>

<sup>7</sup> IT News 2022, *50k customers caught up in Spirit Super phishing attack*, <https://www.itnews.com.au/news/50k-customers-caught-up-in-spirit-super-phishing-attack-580647> 50,000 members were affected.

<sup>8</sup> NGS Super, *Cyber incident update*, <https://www.ngssuper.com.au/articles/news/cyber-incident-update>. NGS Super did not report the number of members affected, but had 114,490 members as of June 2023.

<sup>9</sup> Super SA, *Important information – third-party provider cyber security incident*, <https://www.supersa.sa.gov.au/about-us/announcements/2023/external-provider-cyber-security-incident>. 14,011 members were affected.

<sup>10</sup> IDCare, *Data breaches and scam risks*, <https://www.idcare.org/fact-sheets/data-breaches-and-scam-risks-what-you-need-to-know>

<sup>11</sup> Super Consumers Australia 2023, *Super Consumer Pulse Wave 0*, <https://www.superconsumers.com.au/super-consumer-pulse-blog>

Each super scam victim has been robbed of some or all of their retirement savings. Super scams cost consumers their futures and financial wellbeing. They also cost the super industry in lost investment, administration, and dispute resolution fees, and the Australian Government in lost taxation revenue. Significant cost savings and better scam prevention will result from a code coordinating efforts to combat super scam activity.

Drawing from international examples, there are common sense system fixes that the super industry could adopt to make it harder for scammers to steal people's super, and to send a strong message that Australia is not an easy target for scam activity. However, these require a degree of collaboration and adoption that the industry has not yet initiated. It is therefore essential that the government takes further steps to incentivise super funds to fight scams.

Super funds alone cannot stop super scams, but they are the first port of call for money leaving the super system. Super funds play an important part in the scams ecosystem because they are uniquely situated to approve and vet rollover and benefit payment requests.

We endorse Consumer Action Law Centre, ACCAN and CHOICE's joint submission to this consultation in full, including the mandatory bank reimbursement model. Our submission will address Question 6 of the consultation paper – *What future sectors should be designated and brought under the Framework?* We will also provide comments on enforcement and external dispute resolution for a super anti-scam code.

## 1. Super funds should be the next in line for an industry anti-scam code.

Requiring super funds to prevent, detect, disrupt and report scams will be integral to safeguarding members' savings, dissuading scammers from targeting super, and maintaining the stability and security of the super system as a whole.

There are no specific consumer protections that require super funds to respond to scams in a particular way, despite extensive evidence that demonstrates the need for reform. A number of recent AFCA determinations demonstrate that trustees' broad obligations to 'exercise a prudent degree of care, skill and diligence'<sup>12</sup> and act 'efficiently, honestly, and fairly'<sup>13</sup> do not provide sufficient guidance to industry on how to efficiently and effectively mitigate scam harm.

To their credit, some trustees halt SMSF rollover requests if they identify a scam risk. However, AFCA determinations about rollover complaints showcase examples of unreasonable delays, underdeveloped processes, and poor documentation management when trustees are identifying and responding to suspected scam risks. There is a need the need for regulatory clarity.

---

<sup>12</sup> Superannuation Industry (Supervision) Act 1993, section 52A(2)(b) (Cth)

<sup>13</sup> Corporations Act 2001 Section 912A(1) (Cth)

For example:

- **AFCA case 912282:**<sup>14</sup> A trustee did not have sufficient information to initiate a member's SMSF rollover, and identified a scam risk. After additional information was provided by the member, the trustee still did not initiate the transfer, nor did it inform the member more information was required or reply to the member's requests for an update on the transfer. AFCA found the trustee delayed for 3 months, made information requests that were not reasonable or necessary, and required the member to initiate a new rollover application which was also unnecessary.
- **AFCA determination 942285:**<sup>15</sup> A member requested an SMSF rollover but provided incomplete information. Upon receipt of the correct information, the trustee delayed initiating the rollover for an extra week with no explanation, causing losses according to the member. In the trustee's own words, 'There are no specific timeframes for transaction processing if the entity believes, and can substantiate, that the delay was due to additional due diligence requirements.' The trustee indicated the delay was due to an identified scam risk, but according to AFCA, the trustee could not satisfactorily explain the basis on which it identified that risk.

The depth of harm caused super scams and evidence of trustees' inconsistent scam responses demonstrate the need for regulatory clarity. The super industry should be the next area of focus for an industry anti-scam code under the Competition and Consumer Act 2010 (CCA).

## 2. A super anti-scam code should place obligations on super funds, and administrators where relevant, to take steps to identify and disrupt investment scams.

A super anti-scam code will both provide the public with an added layer of scam protection, while ensuring minimum standards are in place for how funds can effectively and efficiently prevent and disrupt scams.

In order to prevent and disrupt scams involving super, a super anti-scam code should:

1. **Require super funds<sup>16</sup> to adopt advanced and effective scam monitoring systems.** Funds should employ new technologies to monitor and flag suspicious activities, transactions, and patterns associated with the super system. They should also report publicly about strategies deployed (without sharing information that is useful to scammers) and outcomes achieved.
2. **Prevent investment scams by requiring super funds to gather certain information, for example whether a person was pressured, about SMSF rollover requests and unusual transactions,** and proactively intervene where red flags are raised.

---

<sup>14</sup> AFCA 2023, *AFCA determination 912282*, <https://service02.afca.org.au/CaseFiles/FOSSIC/912282.pdf>

<sup>15</sup> AFCA 2023, *AFCA determination 942285*, <https://service02.afca.org.au/CaseFiles/FOSSIC/942285.pdf>

<sup>16</sup> Some super funds and trustees outsource functions to administrators. When we say super funds, we mean the entities responsible for administration of super member accounts.

3. Ensure super fund staff involved in preventing, detecting or responding to scams have **sufficient and ongoing training** to perform their duties effectively.
4. Compel super funds to **resource customer service centres appropriately** to respond to member queries and complaints about scams, fraud, and identification issues. This should include mechanisms to deliver quick responses when there is opportunity to clawback scam losses, as well as arrangements to support consumers who may be vulnerable (for example, interpreter services for people who don't speak English as a first language).
5. **Require super funds' participation in information sharing networks** such as the Fintel Alliance, Australian Financial Crimes Exchange, and the National Anti-Scams Centre to help identify and respond to emerging scam and fraud risks.
6. **Require super funds to provide support services for victims, for example, referral to IDCare, and offer pathways for consumer redress**, including reimbursement where consumer protections are not met.

### Lessons from the UK

We propose that a super anti-scam code should take a similar approach to SMSF rollover requests and unusual lump sum benefit payment requests as is taken in the UK.

Prior to 2017, pension scams were estimated to make up 1 in 10 of all pension transfer requests, with an estimated £19 million lost to suspected pension scams between 2015 and 2016.<sup>17</sup> Following a 2016 review, the UK's Department for Work and Pensions initiated three interventions aimed at tackling pension scams. These were:

1. a ban on pensions cold calling,
2. restrictions around pension transfers, and
3. making it harder for fraudsters to open pension accounts.

In 2021, the UK Government introduced the *Occupational and Personal Pension Schemes (Conditions for Transfers) Regulations 2021* which created conditions a pension transfer must meet before it can be approved, giving trustees power to intervene where they have concerns about a potential scam.

Under the regulations, trustees are required to collect information about the transfer request to identify whether any 'amber' or 'red' flags are present – for example, whether the member is seeking to transfer a pension into unregulated or high risk investments. To accompany the regulations, trustees are provided with guidance on the types of questions they should ask members to identify scam risk, including:

- Did someone advise or recommend that you consider a pension transfer?
- Were you first approached by email, text, phone call, letter or through social media (for example Facebook or LinkedIn) or in person?

---

<sup>17</sup> Department of Work and Pensions 2017, *Pensions scams: consultation*, <https://www.gov.uk/government/consultations/pension-scams/pensions-scams-consultation>

- Do you feel you were put under any pressure to make a quick decision about the transfer?
- When contacted were any of the following terms used by those who approached you?
  - an offer of ‘a free pension review’
  - early access to cash, access to some or all of your pension savings before age 55 (normal minimum pension age), or a savings advance
  - a ‘time limited’ offer.

Depending on the information a member provides, the transfer request is categorised as containing green, amber or red flags. High risk transfer requests are halted and members are referred to the government’s Money and Pension Service.

According to a 2023 review of the new regulations, approximately 1% of pension transfers had an amber or red flag over a period of 18 months, requiring industry follow-up. Based on trustee and Money and Pension Service data, the UK Government estimates that approximately 2,000 potential scam transfers were halted by the red and amber flag system between December 2021 and February 2023.<sup>18</sup>

### 3. A super anti-scam code should be enforceable by ASIC.

The consultation paper proposes a joint regulator model in which the ACCC enforces high level scam obligations in the CCA, and the relevant regulator of each sector enforces the corresponding industry code. In order to be consistent with other aspects of the Australian Consumer Law, ASIC should be tasked with enforcing both the high level scam obligations and anti-scam codes in financial services contexts, including super.

### 4. It should be clear where consumers can go for help with a super scam, and AFCA should be able to hear all complaints relating to scam losses.

Under the proposed framework in the consultation paper, it is unclear how a consumer should seek redress for a super scam. We have outlined an example scenario below.

---

<sup>18</sup> Department of Work and Pensions 2023, *Review of the Occupational and Personal Pension Schemes (Conditions for Transfers) Regulations 2021 (SI 2021/1237)*, <https://www.gov.uk/government/publications/conditions-for-transfers-regulations-2021-review-report/review-of-the-occupational-and-personal-pension-schemes-conditions-for-transfers-regulations-2021-si-20211237>

### **Example scam scenario: Maria and Eddy**

Maria has a social media account and receives a targeted ad from a finfluencer named Eddy promising a lucrative superannuation investment opportunity. Maria sends a direct message on the social media platform expressing interest in the opportunity. Eddy replies to Maria and promises to take Maria on as a client as long as she signs up today. He gives her a phone number and email address to contact him on. Maria checks the Australian Financial Services Licence (AFSL) Eddy gave her on ASIC's website – it looks legitimate.

Eddy tells Maria to set up an SMSF and transfer her super into it, which she does – it's about \$100,000. Eddy coaches her through setting up an SMSF and helps her navigate all the forms. Maria's super fund does not ask any questions about the SMSF transfer request, and approves it a few days later. Eddy then asks Maria to transfer her super in instalments to the bank account of Eddy's investment firm, Make Money Fast Inc, which she does over a few weeks.

A few months later, Maria gets back in touch with Eddy to see how her super is tracking. She doesn't hear back. Eddy's social media account has been closed, his phone cut off, and his email address bounces back. Maria's money has been stolen.

It is unclear who Maria should complain about and where she should complain to under the proposed regulations. The social media platform allowed Eddy to place targeted ads. Eddy appeared to have a valid AFSL, and a phone service he was using to perpetrate the scam. The super fund didn't ask any questions about the SMSF transfer. The bank didn't query the series of transfers.

There should be a 'no wrong door approach' to scam complaints. We support the model proposed in Consumer Action Law Centre, ACCAN and CHOICE's joint submission to this consultation, in which scam losses are reimbursed by the consumer's bank within 5 business days and liability for scam losses are apportioned after the fact by relevant industry members. In Maria's example, this would be between the social media platform, the super fund, the telco and the bank. Under this model, AFCA should be able to hear all complaints relating to scam losses.

### **5. CCA scam obligations should be clear on how businesses should respond to scam complaints.**

We are broadly supportive of the proposed ecosystem-wide enforceable obligations in the CCA, particularly those relating to firms' need to develop an anti-scam strategy. With regards to the 'Response' obligations, we have the following recommendations.



## Contactability

Obligation 2 requires a business to have a mechanism by which consumers can report a scam. Unfortunately, many super funds have issues with contactability. It is not uncommon for a member to go days and weeks without receiving a phone or email reply from their fund about an issue or inquiry.

A requirement to have a mechanism to report a scam does not require businesses to be responsive or explicitly contactable. We recommend updating the wording to the following:

*A business must have user-friendly, effective, efficient, transparent, and accessible options for consumers or users to report a scam, including people not directly targeted by a scam. **A business must be contactable and responsive to scam reports within 2 business days.***

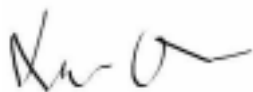
## Complaints handling

A consumer should not have to make a formal complaint in order to get an issue or enquiry resolved. Many consumers do not even realise they are able to make a formal complaint about a business in many instances. Many others do not have the time or capacity to participate in internal and external dispute resolution (IDR and EDR) processes, or may be discouraged from doing so because they think it is unlikely to go anywhere. By articulating businesses' responses to scams within the frame of IDR and EDR, there is a risk only the most engaged and assertive consumers will have their scam issues resolved.

Obligation 4 poses that when a consumer *escalates concerns* with a business, they should be dealt with fairly and promptly, and consumers should be given access to information about dispute resolution options where applicable.

In keeping with RG271's definition of a complaint, '**escalate concerns**' should be replaced with '**expresses dissatisfaction**' to capture a broader range of consumer interactions, and ensure any consumer dissatisfaction is addressed properly.

Thank you for the opportunity to provide comments. Please contact Super Consumers Policy Manager Rebekah Sarkoezy at [rsarkoezy@superconsumers.com.au](mailto:rsarkoezy@superconsumers.com.au) if you wish to discuss our views further.



**Xavier O'Halloran**

Director, Super Consumers Australia