Australian Government

National Anti-Scam Centre

ASIC
Australian Securities & Investments Commission

Investment scam fusion cell

Final report

May 2024

Acknowledgment of country

The ACCC acknowledges the traditional owners and custodians of Country throughout Australia and recognises their continuing connection to the land, sea and community. We pay our respects to them and their cultures; and to their Elders past, present and future.

Australian Competition and Consumer Commission
Land of the Ngunnawal people
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

ACCC 05/24_24–20

www.accc.gov.au

Foreword

We are pleased to present the Investment Scam Fusion Cell Final Report which demonstrates what can be achieved when government, law enforcement and industry take a coordinated approach to scam disruption.

The Investment Scam Fusion Cell (the Fusion Cell) is the first of 4 fusion cells which will be implemented by the National Anti-Scam Centre between 2023 and 2026 to target priority scam issues. Coordinated by the National Anti-Scam Centre, fusion cells focus the efforts of participants from the public and private sector on creative approaches to disruption. Leveraging Scamwatch intelligence, fusion cells focus on measurable disruption trials and cross-organisational 'learning by doing'.

Consumers impacted by investment scams experience devastating lasting financial and psychological harm. The objectives of the Fusion Cell were to identify investment scam campaigns and their enabling technologies, to block the use of these enablers, and to identify barriers to prevention and disruption. The initiatives developed by Fusion Cell participants have led to meaningful disruption of investment scams, with investment scam reports and associated financial losses trending down since the Fusion Cell commenced. We expect this effect will continue as the National Anti-Scam Centre works with partners to extend the disruptions trialled in the Fusion Cell.

As co-leaders of the Fusion Cell, the National Anti-Scam Centre and the Australian Securities and Investments Commission (ASIC) worked closely together to share data and intelligence to disrupt investment scams. Both agencies extend our gratitude to all participants of the Fusion Cell. The willingness to collaborate, share insights and act quickly on intelligence has helped protect Australians from harmful investment scams.

Catriona Lowe
Deputy Chair, ACCC

Sarah Court
Deputy Chair, ASIC

Contents

Executive summary

In July 2023 the Australian Government launched the National Anti-Scam Centre to combat scams by bringing together expertise and resources from across government, law enforcement, industry, and consumer groups. A key activity of the National Anti-Scam Centre is the coordination of fusion cells. Fusion cells are time-limited public-private taskforces that focus on identifying actions to target specific scam problems. Fusion cells differ from the broader information sharing and education activities of the National Anti-Scam Centre by focusing industry and government effort on a particularly damaging scam problem to trial and accelerate disruption action. The initiatives trialled, and lessons learned assist the National Anti-Scam Centre and its partners to work more effectively together to share data and intelligence; target awareness raising; and take effective scams prevention actions including through ongoing working groups on Emerging Trends, Prevention and Communication, and Data Integration & Technology.

The first fusion cell, focussing on Investment Scams (the Fusion Cell) was targeted to address Imposter Bond and Term Deposit scams and AI Trading Platform scams. The objectives of the Fusion Cell were to identify investment scam campaigns and their enablers, to block the use of these enablers, and to identify barriers to better coordinate scam prevention and disruption.

It commenced in August 2023 and ran for 6 months until February 2024. The Fusion Cell brought together 43 organisations across government and industry.[1] In partnership with ASIC, the National Anti-Scam Centre provided data and case studies for analysis and identified strategies and proof-of-concept exercises for further development by participants.

Key Fusion Cell outputs included:

- Creation of **a direct referral process** for the takedown of scam advertisements, advertorials, and videos resulting in more than 1,000 instances being removed by digital platforms.[2]
- Takedown of **220 investment scam** websites.
- **Diversion of 113 attempted calls** to confirmed scam phone numbers to a recorded warning, preventing potentially millions of dollars in imposter bond and term deposit scam losses.

The Fusion Cell provided improvements in scam prevention which extend beyond the term of the Fusion Cell itself:

- Creation of a Scamwatch feature **to make it easier for individuals to report scam advertisements** visible on social media and search platforms such as Google, Meta and Microsoft.
- **Expansion of recorded warnings** to more telecommunication providers in cooperation with Optus and Telstra.
- Development of **technology for automated referral** of relevant reports to Scamwatch for ASIC's service to takedown investment scam websites.
- Proposal for a 3-month data **sharing trial on investment scam payments** which subsequently commenced in April 2024 and will conclude in June 2024.
- Creation of a **handbook of disruption strategies** to identify and combat artificial intelligence (AI) trading platform scams. The handbook collates insights of Fusion Cell participants and will help to establish consistency in industry understanding of indicators and responses to these scams.

1 A full list of participating organisations is provided at the end of the report.

2 Due to differences across platforms, calculating aggregate metrics of ads removed, ad impressions, and ad clicks on a comparable basis is difficult. The measures provided in this report should be interpreted as indicative estimates as to the likely impact.

This report summarises the Fusion Cell's approach, actions, and achievements during its 6-month term from August 2023 to February 2024, as well as how it will continue to have an ongoing impact. The National Anti-Scam Centre will provide updates on the impact of the Fusion Cell's initiatives in future reports. Work is also underway to identify the area of focus for the next fusion cell, due to commence in June 2024.

Investment scams

Overall losses from investment scams reported to the National Anti-Scam Centre's Scamwatch reporting service, ReportCyber, IDCARE, ASIC and the Australian Financial Crimes Exchange amounted to $1.3 billion in 2023, down from $1.5 billion in 2022.[3] These aggregated figures demonstrate the size of the investment scam challenge and harm to Australians. Currently, Scamwatch data provides more granular data from which the National Anti-Scam Centre can better understand monthly trends and average losses suffered by Australians.[4] In 2023, Scamwatch received over 8,000 reports of investment scams with total reported losses of $292 million, accounting for over 60% of total financial losses reported to Scamwatch. For those people that reported an investment scam loss to Scamwatch in 2023, the average amount lost was around $81,000.

As noted in the *National Anti-Scam Centre quarterly update (Jan–Mar 2024)*, investment scams losses have continued to fall in the January to March quarter 2024, by a further 10.1% to $47.1 million (and down by 47% compared to the corresponding quarter in 2023). This trend is encouraging, and an early sign that industry and government's response to scams is beginning to have impact. However, highly damaging losses continue to fall on Australians seeking investment opportunities.

Figure 1 below shows the trajectory of investment scam losses reported to Scamwatch each quarter since the beginning of 2020. The shaded area represents the time of the Fusion Cell.

Figure 1: Total investment scam losses reported to Scamwatch

Scammers perpetrate a wide variety of investment scams, including fake Initial Public Offerings (IPOs), superannuation scams, Contract for Difference (CFD) scams and foreign exchange scams, imposter bond and term deposit scams, and AI trading platform scams. The Fusion Cell analysed intelligence and case studies which informed a decision to target disruption of 2 types of investment scams: imposter bond and term deposit scams, and AI trading platform scams (these are explained in more detail below). The decision to target these scam types by the Fusion Cell reflected the prominence and high-impact of these scam types, as well as the opportunities these scams presented to test disruption strategies.

3 See Targeting scams: report of the ACCC on scams activity 2023 for an in-depth analysis of scam trends.

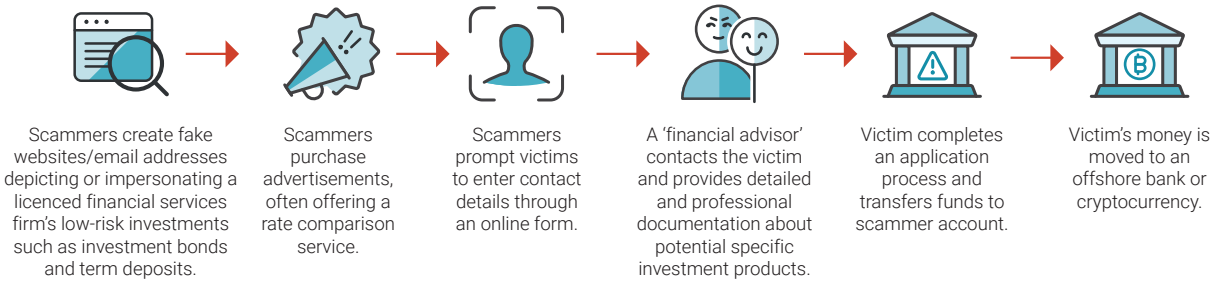
4 The National Anti-Scam Centre is working towards integrating key sources of scams data on a near real-time basis to provide more regular and comprehensive intelligence about scam activity in Australia. More information on the data integration work is available in the *National Anti-Scam Centre quarterly update (Jan–Mar 2024)*.

Imposter bond and term deposit scams

Imposter bond and term deposit scams deceive people into believing they are investing with a legitimate company or bank. People are most often exposed to these scams when they are conducting online research into low-risk investment opportunities, for example, when on digital platforms or searching for market rates for investments in term deposits and bonds.

In 2023, Scamwatch received more than 440 reports of imposter bond and term deposit scams, with total reported losses amounting to more than $41 million. For those that reported a loss, the average amount lost was around $264,000. While the number of reports may seem limited these scams are the highest average loss category and interventions which focus on this scam type have high impact.

How a typical imposter bond and term deposit scam works



Scammers create fake websites/email addresses depicting or impersonating a licenced financial services firm's low-risk investments such as investment bonds and term deposits.

Scammers purchase advertisements, often offering a rate comparison service.

Scammers prompt victims to enter contact details through an online form.

A 'financial advisor' contacts the victim and provides detailed and professional documentation about potential specific investment products.

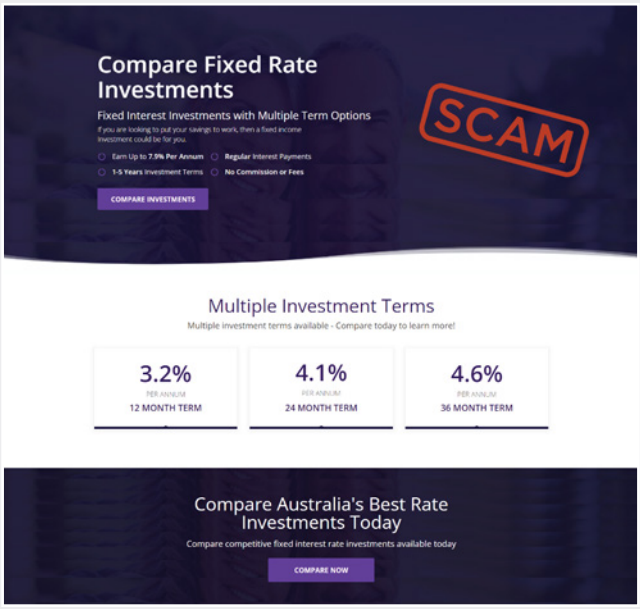
Victim completes an application process and transfers funds to scammer account.

Victim's money is moved to an offshore bank or cryptocurrency.

Case study – Imposter bond and term deposit scam

Claire wanted to open a term deposit. She searched online for the best rates and found a website offering comparative interest rates. She registered her phone number and email address and received a phone call from a man who identified himself as a senior sales manager at a bank. The 'sales manager' had a detailed resume available publicly on an online platform.

Image of an imposter bond and term deposit scam



Claire received an email from the 'sales manager' about fixed term deposits with monthly interest payments. The email and documentation looked professional and over the next few days, Claire provided personal information and ID documents as part of the application process. Claire then transferred $120,000 to the account name and number she was provided.

Claire received credentials for what she believed to be her new term deposit account. The account appeared to show her account balance. Weeks later when she didn't receive an interest payment, Claire contacted the bank she believed she had the fixed term deposit with, who had no record of her account.

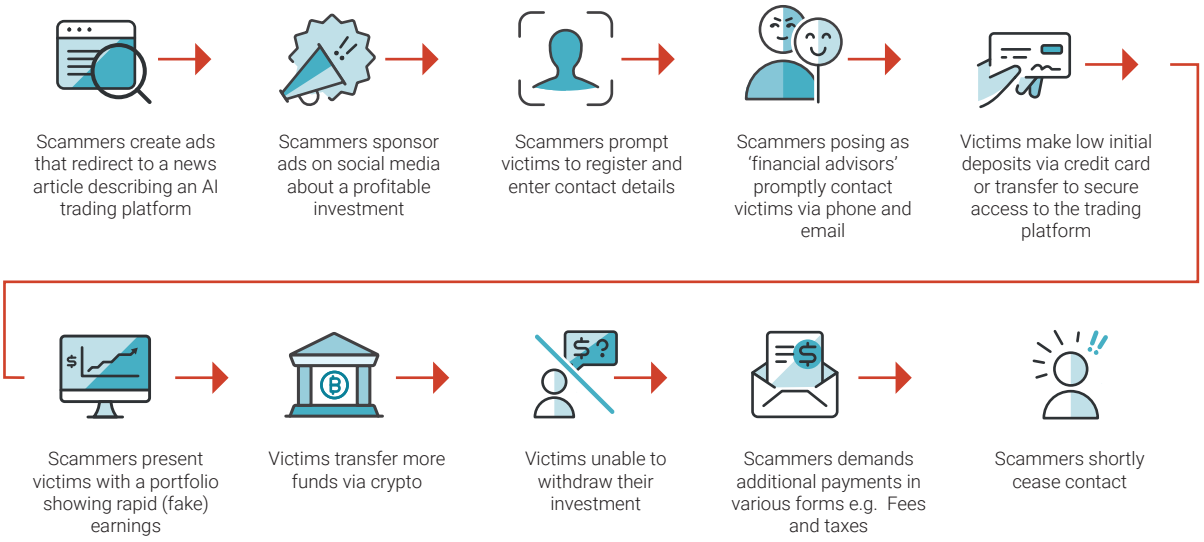
AI trading platform scams

AI trading platform scams claim to leverage AI software and emerging technology to generate high returns with minimal effort or expertise from the investor. These scams often target inexperienced investors who are not actively looking for investment opportunities. They are enticed by advertisements and online news articles featuring fake celebrity endorsements to start online trading, for a low upfront cost. Advertisements promote trading in foreign exchange, contracts for difference (CFD) derivatives, or cryptocurrency and consumers are given access to an online trading platform which appears to show early trading success, followed by losses. Consumers are often given trading credits to 'trade' their way out of illusory losses and then incur an apparent debt which they are required to repay.

Based on conservative estimates, Scamwatch received 400 reports of AI trading platform scams with reported losses totalling more than $8 million in 2023. For those that reported a loss, the average amount lost was around $30,000.

However, the true losses reported in 2023 are likely to be closer to $20 million, with more than 600 reports to Scamwatch featuring common methodology used in AI trading platform scams. Given the increasing prominence of AI, the Fusion Cell considered AI trading platform scams to represent an emerging scam trend requiring urgent disruption.

How a typical AI trading platform scam works



Case study – AI trading platform scam

Louise saw a link on a website indicating a well-known Australian personality had invested in a platform called Quantum AI which the website said was associated with Elon Musk.

Image of a deepfake AI trading platform video

Louise clicked the website link, registered her contacted details, and was connected by a person who helped her register a trading account for her after making a $200 deposit. Louise did some research and the investment website seemed legitimate.

Another person contacted Louise to continue offering trading options. Louise invested another $200. Her trading account appeared to show that Louise was making a profit and over the following days she paid over $8,000 in crypto currency into the trading platform.

Louise's bank contacted her to warn her she had likely been scammed and prevented further payments. Louise tried to withdraw her money from the trading platform, but she was locked out of her 'account' and she could no longer log in or contact anyone for assistance.

Fusion Cell's scam disruption

The National Anti-Scam Centre identified businesses in key sectors and invited them to join the Fusion Cell and collaborate to devise and test disruption strategies at the various stages in the victim's journey through the scam. In this respect, the Fusion Cell embodied the whole-of-ecosystem approach to scams disruption.

Fusion Cell participants analysed case studies developed by the National Anti-Scam Centre to identify risks or system weaknesses and opportunities to disrupt investment scams. The National Anti-Scam Centre shared scam intelligence[5] and convened smaller working groups of participants to develop and test ideas.

Journey of a scam across industry sectors

Step 1

Online inducement

- Digital platforms

Step 2

Engagement and further scam contact

- Telecommunications firms
- Digital platforms

Step 3

Transfer of funds

- Banks
- Digital currency exchanges
- Superannuation & wealth management

Disrupting scam advertisements

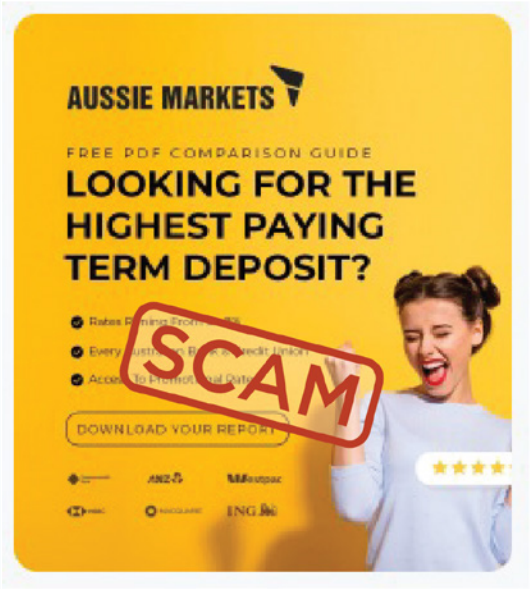
Problem

Advertisements are a primary channel for scammers to make first contact with a potential victim. Advertisements can be found on search engines, social media platforms or as display advertisements in trusted content (such as a legitimate website). There are several obstacles to disrupting scam advertisements:

- Scam advertisements are highly ephemeral. Members of the public see an advertisement and interact with the scam perpetrator but often only become aware of the scam sometime later, after the original advertisement has been removed.
- There is an active contingent of altruistic reporters to the National Anti-Scam Centre's Scamwatch reporting service however, prior to the Fusion Cell, reporters rarely reported actionable intelligence which would enable identification of the initial online inducement.
- While most digital platforms have processes for individual users to report scam advertisements, prior to the Fusion Cell trial there were no well-developed ways for government and private sector stakeholders to refer investment scam advertisements for rapid takedown.

5 This relates to scam vectors i.e. bank accounts, phone numbers, URLs, cryptocurrency wallets, etc. No reporter information was shared unless the reporter had provided specific permissions allowing their personal information to be shared.

Images of imposter bond and term deposit scam advertisements



Opportunities

Fusion cell discussions emphasised the importance of upstream interventions to limit scam contact for the largest number of people. Typically, an advertisement or other online inducement is seen by tens of thousands of people and clicked on by thousands of potential victims.[6] Quickly taking down online advertisements and videos cuts off investment scams at their source.

Actions

The Fusion Cell established direct reporting processes with Google, Microsoft and Meta to take down scam advertisements, advertorials or videos and prevent first contact with the scammer.

Relying on intelligence from participants, reports by the public to Scamwatch, ASIC and ReportCyber, as well as online surveillance by National Anti-Scam Centre staff, the Fusion Cell referred 37 investment scam advertisements and other inducements to platforms for takedown. Digital platform participants conducted analysis to identify advertisement purchasers and related links across all platforms to take down scam advertisements which resulted in over 1,000 takedowns of advertisements, videos, and 'click-bait' advertorials from social media platforms, video sharing platforms, and search engines, such as Instagram, YouTube, Facebook, Yahoo News, Google Search and Microsoft sites.

The Fusion Cell's actions built upon existing scam prevention processes of digital platforms.

6 Based on indicative data provided by participating digital platforms.

Outcomes

While it is difficult to calculate the impact of the advertisement referrals across platforms on a comparable basis, data from platforms indicated these online inducements are visible and clicked on by people extensively, highlighting the importance of removing them as quickly as possible. For example, on average each of the approximately 1,000 instances of scam advertisements removed through the Fusion Cell were potentially seen tens of thousands of times, with thousands of people engaging further by clicking on the advertisements.

These referrals were instances which escaped standard anti-scam strategies used by platforms and therefore helped platforms identify scam practices used to manipulate verification processes, allowing platforms to refine their scam prevention strategies and policies. As the Fusion Cell is a voluntary public/private partnership, participants were not obliged to report on refinements to scam prevention strategies. The Government's forthcoming mandatory industry codes could address this challenge by clear obligations on digital platforms to proactively identify and disrupt scams operating on their platforms and report on actions taken.

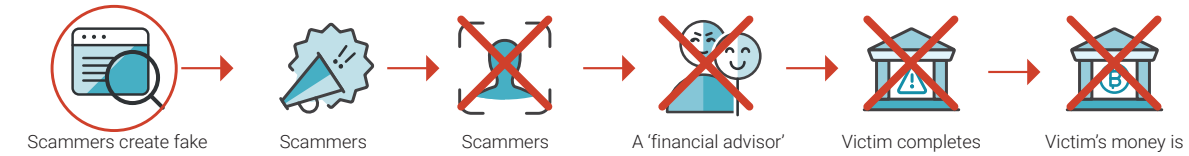
This exercise also identified the limits of current intelligence sources. Advertisements are highly ephemeral and prior to the Fusion Cell reports to Scamwatch rarely included actionable intelligence. Nor were other intelligence sources able to supplement this story. With the right guidance, altruistic reporters can play an important role in supplying timely intelligence which, after evaluation by the National Anti-Scam Centre, can be referred to digital platforms as a 'trusted' report to disrupt scam advertisements.

Future actions

1. The National Anti-Scam Centre has developed a Scamwatch 'short form' for members of the public to report advertisements quickly and easily and capture actionable intelligence for investment scam takedown. The form was developed in consultation with digital platform participants and simplifies the advertisement reporting experience for Scamwatch users. This is expected to be live in June 2024 after development and user testing. The National Anti-Scam Centre will promote the new form and encourage the public to report scam advertisements to Scamwatch as well as directly to the relevant platform, reporting to Scamwatch will aid disruption through referrals by the National Anti-Scam Centre to digital platforms as well as providing the National Anti-Scam Centre with a clearer picture of trending scams on digital platforms.
2. The National Anti-Scam Centre will continue to collaborate with digital platforms on strategies for preventing scam advertisements, including:
    a. creating processes for timely referral of scam advertisements gathered through the new Scamwatch short form to platforms
    b. improving mechanisms for direct consumer reporting. Digital platform responsiveness to direct consumer reports and visibility of that responsiveness would be enhanced by the inclusion of obligations in the forthcoming mandatory code.

Disrupting scam websites

How website takedowns disrupts imposter bond and term deposit scams



Scammers create fake websites/email addresses depicting or impersonating a licenced financial services firm's low-risk investments such as investment bonds and term deposits.

Scammers purchase advertisements, often offering a rate comparison service.

Scammers prompt victims to enter contact details through an online form.

A 'financial advisor' contacts the victim and provides detailed and professional documentation about potential specific investment products.

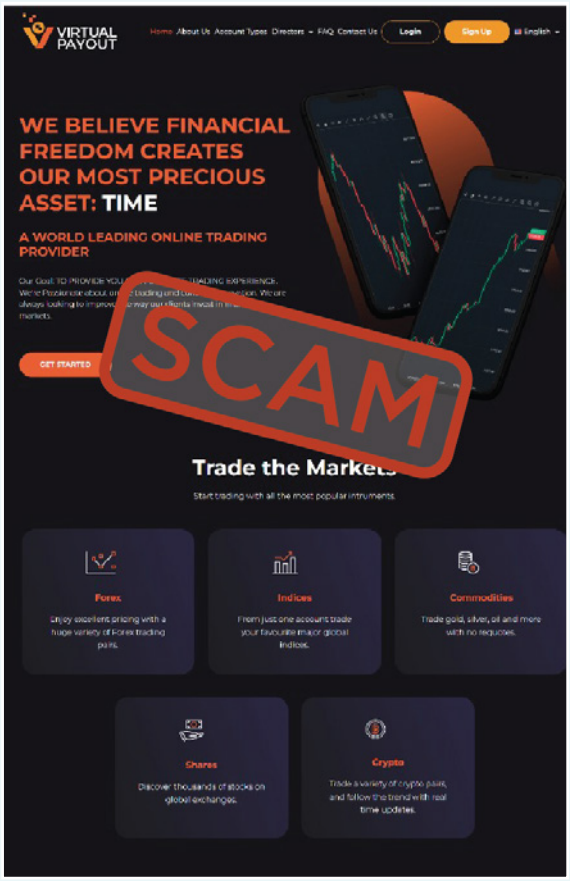
Victim completes an application process and transfers funds to scammer account.

Victim's money is moved to an offshore bank or cryptocurrency.

Problem

Financial criminals use scam websites to deceive people and create the illusion of a legitimate investment opportunity.

Image of AI trading platform scam website



Opportunity

Taking down scam websites reduces scammers' ability to gather contact details, identity documents, and funds from victims. In addition, website takedowns can alert people who are already being scammed, as seeing the website has been taken down may cause them to reach out for assistance.

Actions

In November 2023, the Assistant Treasurer announced ASIC's new scam website takedown capability. ASIC has engaged a cybercrime detection and disruption firm to remove or limit access to investment scam and phishing websites.

As part of the Fusion Cell, the National Anti-Scam Centre asked participants to provide suspected scam websites and referred these to ASIC for takedown evaluation to maximise intelligence available for takedowns.

The National Anti-Scam Centre also established daily referrals of websites reported to Scamwatch to share threats with ASIC within a short period after being reported. Quickly acting on intelligence from the public mitigates the risk of a newly created scam website.

Outcomes

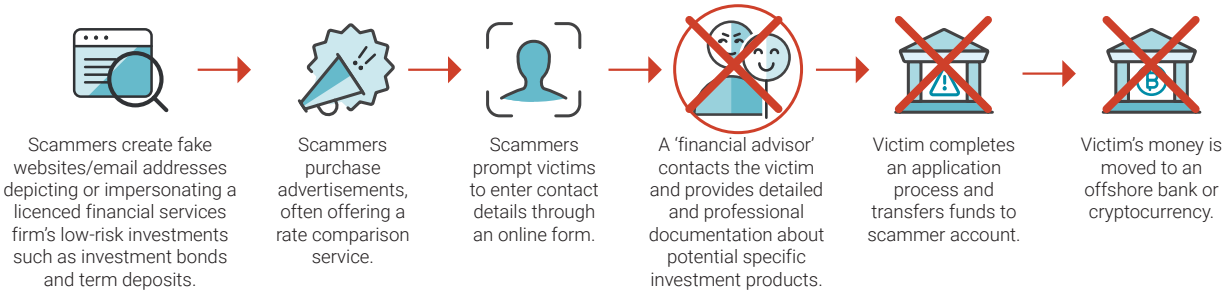
During the 6 months the Fusion Cell operated (August 2023 to February 2024) nearly 4,000 investment scam websites were taken down. ASIC's proactive identification process was supplemented with 1,700 unique URLs from Fusion Cell participants and the National Anti-Scam Centre resulting in a further 220 takedowns. While the contribution of the Fusion Cell participants to overall takedowns was relatively small, these takedowns represent cases which were not being identified by proactive processes and may otherwise have remained live and exposed more Australians to the risk of being scammed.

Future actions

1. The National Anti-Scam Centre is developing a technology solution to automatically refer investment scam websites reported to Scamwatch to ASIC for takedown, which will be launched in the second half of 2024.
2. Given the success of ASIC's takedown service for investment scams, the National Anti-Scam Centre has begun its own website takedown trial covering a broader range of scam websites, such as online shopping and phishing scams. This will complement ASIC's takedown capability, which is limited to investment and financial service scams, consistent with its regulatory responsibilities.

Disrupting phone contact

How call diversion disrupts imposter bond and term deposit scams



Problem

Direct phone contact between scammers and potential victims provides another avenue for scammers to convince a person that an investment scam is legitimate. Through direct conversation, fake 'Advisors' seek to build trust with victims. If a scam phone number is blocked without explanation, perpetrators of investment scams provide plausible reasons for why a number is no longer in use and re-establish contact on another number.

Opportunity

Telecommunication providers are in a unique position to take action to prevent phone contact from scammers. Improving the telecommunication provider's capability to verify that a number is being used to perpetrate an investment scam and subsequently provide recorded warnings to people calling a phone number provided by a scammer can be effective in breaking contact between the victim and scammer and reduce financial losses.

Actions

The Fusion Cell built upon an existing Optus 'Call Stop' initiative which was developed in conjunction with banks and the Australian Financial Crimes Exchange to counter bank impersonation SMS scams where scammers ask consumers to call back a number provided in an SMS.

In the Fusion Cell trial, the National Anti-Scam Centre worked with Fusion Cell members, and other impersonated financial institutions to identify, validate and share confirmed scam phone numbers with Optus. When a potential victim tried to call a confirmed scam number over the Optus network, their call was diverted and the consumer received a recorded warning saying:

> The number you have called has been reported as being used for scam activities.
> For more information, please visit optus.com.au/CallStop.

The Optus website also refers people to Scamwatch for more information and assistance if they have been a victim of a scam. This disruption is unique in that it provides a direct and active warning to a potential victim, rather than a passive signal (removal of a website or advertisement).

Outcomes

The 3-month Optus trial resulted in the diversion of 113 calls that would otherwise have put Australians in contact with financial criminals pretending to offer legitimate investment opportunities. The average loss reported to Scamwatch in 2023 for an imposter bond and term deposit scam was around $264,000, so it is estimated that this trial prevented millions of dollars in losses.

Future actions

1. The National Anti-Scam Centre will continue to refer confirmed scam numbers to Optus for diversion to recorded warnings.
2. The National Anti-Scam Centre will work with telecommunication providers during 2024 to expand recorded warnings and other solutions to protect their customers from investment scams.
3. The National Anti-Scam Centre will advocate for obligations under the relevant industry codes for the creation of similar customer alert systems to protect more consumers.
4. The National Anti-Scam Centre will escalate confirmed scam numbers to relevant enforcement bodies for evaluation and work with telecommunication providers to implement best practice data acquisition, validation and sharing including exploring improved direct reporting by consumers to their telecommunication provider.

CASE STUDY – Fusion Cell call diversion trial averting losses

David was looking to invest a lump sum in a term deposit. David researched online the best term deposit rates available and registered interest on several sites. He was contacted by an individual claiming to work for a well-known financial institution. After corresponding David decided to invest $300,000. He completed an application form and received 'approval' as a new customer.

Prior to making the financial transfer, David had a question about the application process and called the number he was provided by his 'advisor'. Fortunately, this number had been identified through Scamwatch and the National Anti-Scam Centre provided it to Optus for incorporation into Call Stop. This enabled Optus to warn its customers when they made a call to an identified scam number, and other telecommunications providers blocked this number.

Because David was an Optus customer, when he attempted to call the number, he heard a recorded warning that the number had been used as part of a scam. David ceased his interaction with the scammer, independently sourced a phone number for the impersonated financial institution and found they had no record of his application. David lodged a report with Scamwatch, which helped the National Anti-Scam Centre to report his experience. Warnings rather than simply blocking calls help potential victims to permanently break contact with the scam perpetrator.

Disrupting scam payments

Problem

Investment scams play out over a period of weeks or months and a lengthy period can elapse before a consumer discovers they have been a victim of a scam, by which stage the funds they have transferred have likely been moved offshore, often into cryptocurrency.

Opportunity

Sharing information and strategies across sectors in the Fusion Cell, particularly between banks and digital currency exchanges, can help to identify payment methodologies used by scam perpetrators and reduce the accumulation of financial losses.

Actions

A working group was formed involving Mastercard, Commonwealth Bank, Westpac and CoinSpot to examine disruption strategies for scam payments (*Payments Working Group*). This working group identified key intelligence which could be shared using existing sharing arrangements for financial services via the Australian Financial Crimes Exchange. A 3-month proof-of-concept trial was formulated toward the end of the Fusion Cell to identify and disrupt scam payments. The trial extends from 11 March to 11 June 2024.[7]

A working group was formed by NAB, Macquarie Bank, CoinJar, Australian Payments Network, ANZ, Vanguard, ASIC and Crypto.com (*Disruption Handbook Working Group*) to capture and record strategies for identifying and preventing scam payments in a handbook focused on AI trading platform scams.

Outcomes

The disruption handbook for AI trading platforms is a voluntary resource that will help to create consistency in how organisations respond to AI trading platform scams. The handbook includes guidance for automated transaction monitoring systems and customer due diligence processes including the use of forms and screening steps for detecting potential scam victims. Organisations naturally differ in their approaches to scam prevention and the handbook will support greater consistency in ecosystem responses to scam payments by sharing information about disruption protocols. Initially the handbook will be shared with Fusion Cell participants but after a later evaluation exercise (discussed below), the National Anti-Scam Centre will consider broader dissemination – noting the handbook contains sensitive information which should not be inadvertently made available to scammers.

7 Ideation occurred over several months during the Fusion Cell. This trial was considered viable but required research by working group members to adequately prepare for the trial, which could not occur before the end of the Fusion Cell.

Future actions

1. In conjunction with the National Anti-Scam Centre, the Payments Working Group will evaluate the success of the payments intelligence sharing proof-of-concept trial and, if successful, develop a plan for implementation and broader adoption.
2. In conjunction with the National Anti-Scam Centre, the Disruption Handbook Working group will establish a focus group to assess whether the document is fit-for-purpose and has been adopted in practice by Fusion Cell participants and implement an action plan for feedback.

Awareness and prevention

While the focus of the Fusion Cell was on strategies to take down online scam inducements and websites, and to disrupt scam payments, the Fusion Cell members also discussed the importance of targeted awareness in disrupting investment scams and contributed to ongoing efforts in this regard.

The Fusion Cell noted the diverse range of methods for alerting the community, including ASIC's new investor alert list, launched in November 2023. The investor alert list helps inform consumers about investments that could be fraudulent, a scam or are being offered and promoted by unlicensed entities and individuals. It also includes 'imposter' entities, which impersonate or falsely claim to be associated with a legitimate business (impersonation scam). The investor alert list is used by organisations including the Australian Financial Crimes Exchange, banks, and other financial services to update their scam detection systems with current information about companies and businesses that are not to be trusted enabling them to better protect their customers by flagging potential scam transactions, as well as being an authoritative information source to support advice to customers that they should stop sending payments. Legitimate financial advisers can also use the investor alert list to provide advice to protect their customers from investment scams.

> Since its launch, ASIC has added more than 500 new entries on the investor alert list. More than 220 of these entries were reported to ASIC by members of the Fusion Cell. The investor alert list webpage has had over 91,000 page views since its creation.

Consumers can search the investor alert list by visiting https://moneysmart.gov.au/check-and-report-scams/investor-alert-list and listings will also appear in search engine results when consumers look up the name of an entity appearing on the list. This is important as it means consumers don't need to know about Investor Alert in order to receive a warning.

Similarly, authoritative information about scam methods can allow consumers to match their experience against that described by a trusted source. ASIC and the National Anti-Scam Centre issued a joint media release about AI trading platform scams (It's a scam! Celebrities are not getting rich from online investment trading platforms | ACCC) and a scam alert was published on the Scamwatch website Scam alert: Fake celebrity online investment scams.

CASE STUDY – Fusion Cell contribution to scam awareness and prevention

Sam was browsing an online marketplace looking for a good bargain when she came across a sponsored advertisement about investing. The advertisement appeared to be legitimate as the image included a well-known news site and TV presenter.

After clicking the advertisement, Sam was redirected to an investment website promoting a new AI trading software that promised good returns without trading experience. Sam was intrigued as she had never come across an AI trading platform before.

Sam quickly googled "Quantum AI scam" to see if there was anything online about it. On the first page of Google search results was the ACCC's public release describing Quantum AI as a scam. Sam immediately knew it was a scam and reported her 'near miss' via Scamwatch. The release, leveraging the work of the Fusion Cell, stopped Sam from potentially losing money.

Scam alert: Fake celebrity online investment scams

1 Mar 2024

Background

Fake news and 'deepfake' videos of celebrities and public figures appearing to promote online investment platforms are increasing on social media.

'Deepfakes' are lifelike impersonations of real people created by artificial intelligence (AI).

Scammers create ads and fake news articles to get you to believe the celebrities actually use these scam investment platforms.

The platforms claim to use AI and other technologies like quantum computing to create high profits for investors.

Subscribe for email alerts on the latest scams.

Subscribe to email alerts

Evaluation of the Fusion Cell

The Fusion Cell was a first-of-its-kind initiative designed to address the urgent problem of investment scams on an ecosystem basis. 'Learning-by-doing' was a key principle of the Fusion Cell and this principle also relates to the operation of the Fusion Cell format itself. The learning curve of the first fusion cell provides an opportunity to act on feedback and observations for future fusion cells.

At the end of the Fusion Cell, the National Anti-Scam Centre surveyed participants seeking feedback on the Fusion Cell. 16 responses out of 43 participants were received. While this response rate was disappointing, it is reflective of the proportion of active participants in the Fusion Cell. **A small proportion of participants committed whole-heartedly**, while others appeared to be waiting for the Fusion Cell to prove the efficacy of proposed initiatives or chose to observe rather than commit to action.

Some respondents noted the need for a stronger focus on **tangible outcomes** with objectives agreed upfront to ensure all stakeholders **commit equally**. Others noted the difficulty in participating given the size of the Fusion Cell. The formation of **small working groups** in the latter half of the Fusion Cell was highly effective in securing active participation and converting high-level discussion into tangible outputs. The emphasis on **proof-of-concept exercises** was also helpful in establishing efficacy before committing ongoing resourcing, which is a valid consideration for participants.

Respondents noted the brevity of the Fusion Cell given the breadth of the topic and that the **timeframes limited the execution and delivery of disruption outcomes**, with one respondent noting that "…the prevalence of investment scams demands a more prolonged timeframe for comprehensive execution". This is a valid observation, although early refinement to 2 damaging scam types mitigated this issue.

Some respondents expressed concern about the measurability of success. In the absence of controlled trials, measuring the effectiveness of specific initiatives in numerical terms is challenging. While the *National Anti-Scam Centre quarterly update (January to March 2024)* notes the strongest decrease in scam losses has been in investment scams, the breadth of measures taken by Government and industry in the last year[8], render it difficult to isolate causality. Nonetheless, establishing the counterfactual for what would have occurred in the absence of future fusion cells will be helpful for evaluation of those future fusion cells. The National Anti-Scam Centre is giving consideration to how best to do this ahead of the next fusion cell.

Respondents provided a range of comments noting the benefit of bringing representatives from different sectors together to share actionable intelligence and discuss disruption strategies.

> "The Fusion Cell represents a quantum leap in promoting a public-private partnership to combating and disrupting scam and fraud activity. It effectively replaces the patchwork and club-like approach that preceded it …."
>
> "…the ability to share information, discuss campaigns and systems, and getting 'the right people in the room' made a huge difference"

From the National Anti-Scam Centre perspective, participation from sectors which intersect with the full length of the victim's journey was beneficial for creating **a sense of shared responsibility**.

8 For example, actions taken in mid-2023 to restrict the access of a major digital currency exchange, Binance, to Australian payment systems and the imposition of frictions on cryptocurrency payments by various banks is likely to have a measurable effect.

Considering this feedback, along with the National Anti-Scam Centre's own observations, future fusion cells will emphasise the following features:

- Greater time in **establishing scope** prior to the fusion cell initiation, with consideration to what is achievable in fusion cell timeframes.
- Reliance on **small working groups** and emphasis on **proof-of-concept exercises**.
- **Terms of reference** which require participants to report on the **additionality** of the fusion cell activities to establish a counterfactual scenario.
- **Greater emphasis on benchmarks for success** in the initial weeks of the fusion cell.

The National Anti-Scam Centre considers the merits of the Fusion Cell far outweigh its limitations but will expect more proactive participation from industry in future. Passivity on the part of some participants reiterates the need for mandatory obligations on industry to counter scams. As Australia moves to a mandatory codes framework **businesses must invest significantly in scam countermeasures** and industry should view voluntary initiatives as a stepping-stone to meeting its future mandatory obligations.

Barriers to disruption and possible solutions

An objective of the Fusion Cell was to identify barriers to disruption. Appropriately, Fusion Cell discussions frequently addressed systematic barriers. Many participants highlighted the need for **greater clarity on legal uncertainties relating to privacy and data sharing**.

Participants also highlighted the need for **data sharing infrastructure** to enable disruption actions, although some participants identified integration costs as an impediment to participation in existing industry based data sharing forums. Sharing of **tainted crypto currency wallets** and **encrypted sharing of compromised IDs** were noted as areas of focus for data sharing.

The Fusion Cell also generated a range of valuable ideas which were out of scope or not achievable with the Fusion Cell timeframes, including:

- A **national media campaign** to raise public awareness in relation to scams.
- **Psychological research** to better target messaging and interventions to prevent victimisation.
- The work of industry in scam disruptions should be **partnered with law enforcement** to maximise the potential for prosecution of criminal activity.
- Strategies are needed for promptly **preventing access to scam websites** while voluntary takedown requests are in progress.
- Development of **a retrospective alerting capability** by digital platforms for individuals who have interacted with an online inducement to a scam (for example, an advertisement).

Response

Government

The Australian Government continues to invest in making Australia a hard target for scammers. The Government's **economy-wide agenda** to combat scams will help to address these barriers, through strengthened protections, awareness and support for consumers and business.

In the 2024–25 Budget the Government provided **a further $67.5 million** to continue action to combat scams and online fraud. The funding builds on Government's earlier action to establish the National Anti-Scam Centre, establish the SMS sender ID register and invest in ASIC's website takedown capability. The 2024–25 Budget provides:

- $37.9 million (and $8.6 million ongoing) to introduce legislation to establish and enforce **a Scams Code Framework**
- $6.3 million for the Australian Competition and Consumer Commission to deliver a **consumer education media campaign**
- $23.3 million to support the adoption of eInvoicing to **disrupt payment redirection scams**, improve cash flow and boost productivity for small businesses.

The National Anti-Scam Centre

The National Anti-Scam Centre's development of data-sharing infrastructure directly addresses a key concern with near real-time data sharing capability from July 2024. The National Anti-Scam Centre's growing **partnerships with law enforcement** – primarily via our relationships with the Joint Policing Cyber Crime Centre and ASIC – have created a regular exchange of scam intelligence to inform enforcement prioritisation by relevant law enforcement agencies.

Industry must match this commitment with strong action against scams and help to re-establish public trust in digital infrastructure and services. The National Anti-Scam Centre looks forward to future fusion cells and seeing the fruits of private/public partnerships to the benefit of all Australians.

Fusion Cell participants

The ACCC and ASIC give particular thanks to the following organisations for significant contribution to the Fusion Cell by participation in working groups, pilot initiatives, or other material contributions:

> Optus, Symbio, TPG, Telstra, NAB, Commonwealth Bank, Macquarie Bank, CoinJar, Coinspot, Crypto.com, Mastercard, Westpac, ANZ, Australian Payments Network, and Vanguard.

We would also like to thank Google, Bendigo & Adelaide Bank, BTC Markets, Chainalysis, and Swyftx for chairing discussions, presentations and sharing analysis.

The organisations that attended the Fusion Cell meetings are listed below:

- Australian Communications and Media Authority
- AMP
- ANZ
- Apple
- Australian Federal Police
- Australian Financial Crimes Exchange
- Australian Payments Network
- Australian Taxation Office
- Australian Transaction Reports and Analysis Centre
- Bendigo and Adelaide Bank
- BTC Markets
- Chainalysis
- Class
- CoinJar Australia
- CoinSpot
- Commonwealth Bank
- Crypto.com
- Google
- HSBC Bank Australia
- HUB24 Limited
- Independent Reserve
- ING Bank Australia Limited
- Insignia Financial
- LinkedIn
- Link Group
- Macquarie Bank
- Mastercard
- Meta
- Microsoft
- NAB
- New South Wales Police
- Northern Territory Police
- Optus
- Queensland Police
- South Australian Police
- Symbio
- Swyftx
- Telstra
- TPG Telecom
- Vanguard Investments Australia
- Victoria Police
- WA ScamNet
- Westpac

Appendix: notes on data and case studies in this report

The data in this report is calculated on a calendar year basis, unless otherwise indicated.

Except where specified, all data is based on reports made to the National Anti-Scam Centre's Scamwatch service. Data may be adjusted throughout the year because of quality assurance or changes to categories. While effort is made to verify high loss reports, reports are unverified. Detailed data on scams is published on the Scamwatch website.

Case studies are used throughout the report to illustrate how the National Anti-Scam Centre's work with partners across government, law enforcement and industry is protecting Australians from ever-more technically sophisticated and callous scams. All case studies have been adjusted to protect the privacy of reporters, including by changing names. The National Anti-Scam Centre has also been mindful not to publish information that could assist scammers to counter prevention and disruption efforts.


Australian Government


National
Anti-Scam
Centre