Australian Government

National Anti–Scam Centre

Job Scam Fusion Cell Final Report

May 2025

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

Important notice

The information in this publication is for general guidance only. It does not constitute legal or other professional advice, and should not be relied on as a statement of the law in any jurisdiction. Because it is intended only as a general guide, it may contain generalisations. You should obtain professional advice if you have any specific concern.

The ACCC has made every reasonable effort to provide current and accurate information, but it does not make any guarantees regarding the accuracy, currency or completeness of that information.

Parties who wish to re-publish or otherwise use the information in this publication must check this information for currency and accuracy prior to publication. This should be done prior to each publication edition, as ACCC guidance and relevant transitional legislation frequently change. Any queries parties have should be addressed to the General Manager, Strategic Communications, ACCC, GPO Box 3131, Canberra ACT 2601.

ACCC 05/25_25-09

www.accc.gov.au

Contents

Foreword

I am pleased to present the Job Scam Fusion Cell Final Report, summarising the work, learnings, and achievements of the National Anti-Scam Centre's second fusion cell. Fusion cells demonstrate what can be achieved when government, law enforcement, and industry share a coordinated approach to scam disruption. This report details some significant achievements as well as identifying challenges and lessons learned. Both are important to effectively combatting scams.

Job scams were the fastest growing scam type in 2023, and target vulnerable members of our community and people seeking relief from cost-of-living pressures. The impact of job scams can be devastating and is likely significantly underreported by victims. Many job scam victims report that they have lost their life savings as well as money they have borrowed from family and friends. In addition to these financial impacts, victims incur additional harm through the loss of personal information leading to an increased likelihood of future scam losses and identity crime. The cost of a victim's loss of trust in recruitment processes and loss of confidence in their ability to secure meaningful employment is hard to quantify.

The objectives of the Job Scam Fusion Cell were to identify job scam campaigns and their enabling technologies, to block these enablers, and to identify barriers to prevention and disruption. Participants have worked together to share intelligence, disrupt scam enablers, increase public awareness and education, and identify opportunities for improved collaboration and disruption.

The National Anti-Scam Centre extends its gratitude to the 28 participant organisations of the Job Scam Fusion Cell and the staff who represented them. We are thankful for the knowledge and expertise of these partners; both those new to collaboration with the National Anti-Scam Centre and those returning from the Investment Scam Fusion Cell. The National Anti-Scam Centre would like to acknowledge those participant organisations that made significant contributions to the fusion cell, including Swyftx, Crypto.com, Commonwealth Bank, Google, Meta, the Australian Federal Police, and SEEK. The work undertaken by specific organisations is identified throughout this report.

Catriona Lowe
Deputy Chair, ACCC

Executive summary

The National Anti-Scam Centre's Job Scam Fusion Cell commenced in September 2024. A fusion cell is a time-limited taskforce, bringing together government, law enforcement and industry to address a specific scam issue.

Job scams target people seeking additional income and flexible, work-from-home opportunities. The scam type particularly impacts people with low income, those from culturally and linguistically diverse communities, the long-term unemployed, international students and other non-resident visa holders, people living with disabilities, and others with limited employment options.

In 2023, financial losses to job scams grew by 151% compared to 2022. Scamwatch reports for the 2024 calendar year show Australians lost $13.7 million to job and employment scams, with an average loss of $14,470. This is 5.1% higher than the average loss for all other scam types combined.

The harm caused by job scams extends beyond financial loss. Last year, over a third of job scam victims who reported to Scamwatch noted that they had lost personal information. These stolen details are typically used later in other scams or in crimes involving identity theft. There is also a significant risk of revictimisation, including the likelihood of being targeted by recovery scams in which the original scammer or a related criminal group offers to recover funds lost to the initial scam after the victim pays an upfront fee.

An academic review of job scam victim research found that job scams are a significant crime type across jurisdictions and victim experiences worldwide are similar to those in Australia. Globally, support services are limited, and existing education and awareness efforts largely place the burden on individuals to detect scams rather than addressing the broader systemic issues.

The Job Scam Fusion Cell commenced in September 2024 and ran for 6 months until March 2025. Key outcomes of the fusion cell include:

- referral of 836 scammer cryptocurrency wallets to digital currency exchanges (DCEs) for analysis and investigation, leading to blocking and blacklisting of wallets and other actions that assist disruption
- intelligence sharing leading to Meta's removal of approximately 29,000 accounts engaged in job scams in Australian Facebook groups
- 1,850 scam enablers such as websites and scam job advertisements referred for removal
- distribution of a regular keywords and trends intelligence product to Meta, Google, and other online platforms
- significant uplift of awareness and prevention across the tertiary education sector, including equipping universities and international student study hubs for ongoing delivery of scams awareness messaging
- increased awareness of job scams achieved through consumer and stakeholder engagement with fusion cell social media content
- disrupting scammers' impersonation of Australian Government entities such as the Department of Foreign Affairs and Trade, Department of Home Affairs, and APSJobs
- identification and dissemination of disruption processes and required data points to aid future takedowns of scam content on digital platforms
- uplift of Australian business capability to respond to impersonation in scams through a comprehensive guide

- creation of a guide to disrupting Job Scam Payments, offering businesses in the banking, payments, and cryptocurrency sectors practical advice based on the best practices of industry leaders.

Effective collaboration between government and industry is essential for the prevention and disruption of scams. Throughout the term of the fusion cell, the National Anti-Scam Centre invested heavily in building cooperative relationships with digital platforms, especially Meta and Google. The fusion cell also provided new opportunities for the National Anti-Scam Centre to develop cooperative scam disruption efforts with digital currency exchanges, including Swyftx and Crypto.com.

The fusion cell model enables the National Anti-Scam Centre to implement targeted prevention and disruption activities across the scams ecosystem, informed by data from any other part of the ecosystem. Data from victims' experience, Scamwatch and ReportCyber reports, stakeholder knowledge, and participants' intelligence contributes to prevention and disruption interventions with a cumulative impact.

The tertiary education engagement during the fusion cell demonstrates this benefit, with learnings in respect of the victim journey, analytics from Scamwatch reports, and stakeholder experience contributing to complementary prevention activities; a forum for tertiary education stakeholders, a social media campaign aimed at students, and the development of "train the trainer" workshops equipping universities and state/territory government agencies to deliver scams awareness training. This coordinated approach enables the National Anti-Scam Centre to develop and prioritise complementary interventions to significant combined effect.

Fusion cell participants

The National Anti-Scam Centre acknowledges the following participant organisations:

Recruitment

- Adecco
- LinkedIn
- SEEK

Law enforcement

- Australian Federal Police/JPC3
- South Australia Police
- Queensland Police
- Victoria Police

Banking

- ANZ
- Commonwealth Bank
- Macquarie Bank
- Westpac

Telecommunications

- Telstra
- TPG Telecom

Digital platforms

- Google
- Meta
- TikTok

Cryptocurrency

- BTC Markets
- Chainalysis
- CoinJar Australia
- CoinSpot
- Crypto.com
- Swyftx
- TRM Labs

Government, academic & other

- ACCC
- IDCARE
- Myer
- Queensland University of Technology
- Services Australia

Objectives of the fusion cell

The objectives of the Job Scam Fusion Cell were developed to reflect the 3 pillars of the Australian Government's anti-scam strategy, which are prevention and disruption, consumer awareness, and victim support.

Job scams were selected as the National Anti-Scam Centre's second fusion cell topic through an evidence-based process, considering factors including the increase in reported financial losses for job scam victims, the high average losses, the vulnerability of job scam victims with many from culturally and linguistically diverse communities and in younger age groups, and the disproportionate harm experienced by at-risk groups. Financial losses to job scams reported to Scamwatch were increasing more rapidly than many other scam types. The topic also provided an opportunity to better understand a scam that was reaching victims on social media platforms.

The Job Scam Fusion Cell's objectives were:

- to disrupt job scams via:
  - early identification of job scam campaigns and their enabling factors, including digital platforms, fake websites and messaging apps
  - blocking or limiting scammers' ability to use enabling technology, products, and services
  - developing strategies to stop consumers sending funds
  - Implementing awareness and protection strategies to arm targeted communities and demographics
- to promote collaboration and operate as a sandbox for broader disruption strategies and techniques
- to identify and report on any barriers to coordinated scam prevention and disruption.

The Job Scam Fusion Cell also trialled the use of working groups. These smaller groups with focussed interest and expertise met regularly and collaborated on specific prevention, disruption and awareness products to trial during the term of the fusion cell. All participants were members of one or more of the 4 working groups, which were:

- Intelligence Working Group
- Victims Working Group
- Takedowns Working Group
- Payments Working Group.

Fusion cell participants met for the first time, online, on 13 September 2024. On 24 September 2024, an in-person workshop was held in Melbourne where participants joined and participated in working groups. Participants provided positive feedback about the value of holding an in-person workshop early in the fusion cell's term, to bring participants together to share intelligence and discuss how to achieve the objectives of the Job Scam Fusion Cell.

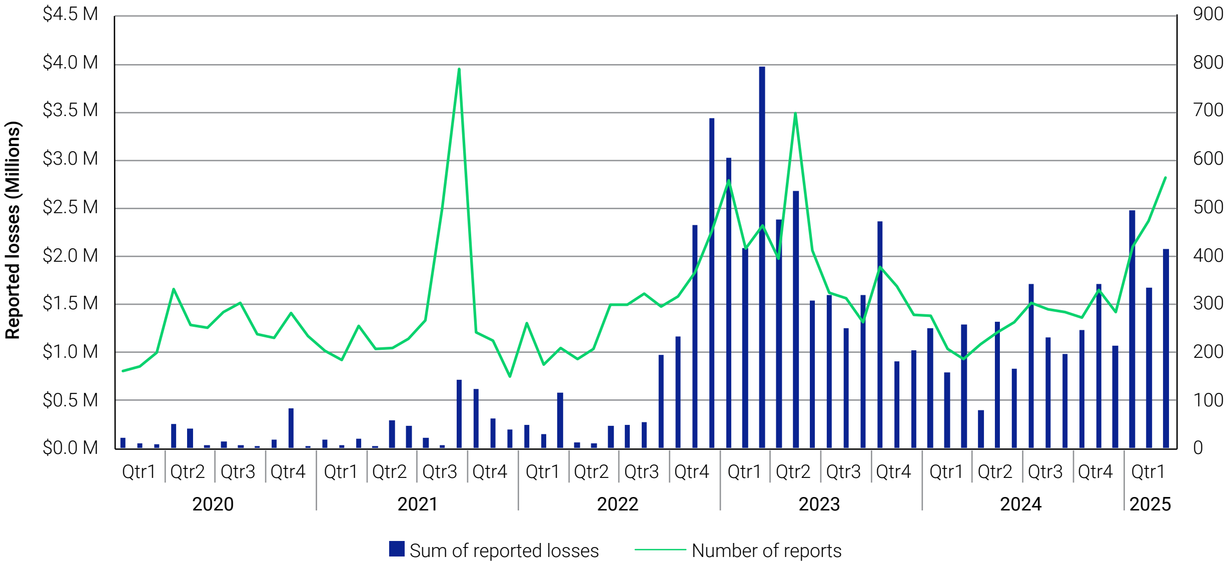
Anatomy of a job scam

In 2024, Scamwatch received over 3000 reports of job scams, with reported losses of $13.7 million. Job scams are often miscategorised within the scam ecosystem, as the methodology involved in the task-based job scam overlaps with other scam types, particularly investment scams.

Total reported losses for job scams are lower than for some other scam types, although the average loss is marginally higher than for other scam types.[1] Furthermore, even moderate financial losses typically have a disproportionate impact. Job scam victims are often unemployed or under employed, and frequently lose all their savings as well as money borrowed from family and friends.

Figure 1 below shows a substantial spike in job scam reports in 2021, followed by a second spike in reports and associated losses in 2022. This increase coincides with the rise of the task-based job scam methodology adopted by scammers.

Figure 1: Job scam losses and reports (Scamwatch, Jan 2020 – Feb 2025)

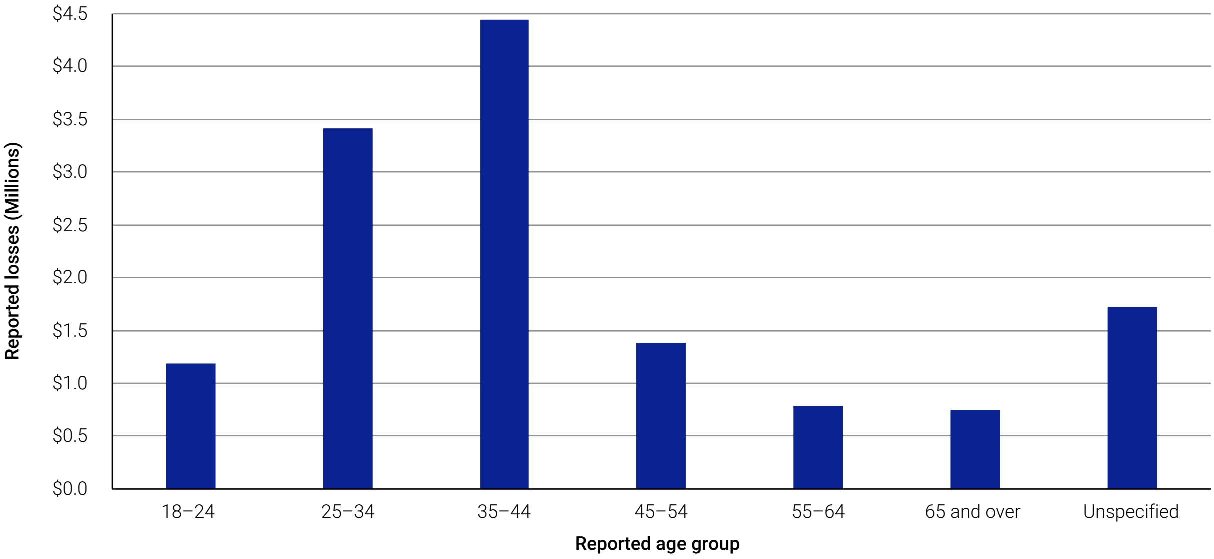


In 2024, 78% of those who provided their age when reporting a job scam were aged under 44. 18.8% of job scam victims who lost money self-reported English as their second language, compared to 7.7% for other scam types.[2] Scamwatch and IDCARE reports indicate that there are slightly more females than males reporting job scams. However, fusion cell participants who proactively contact or are contacted by victims, report that males are more likely to be victims of job scams, but less likely to report.

[1] The average amount lost in 2024 Scamwatch reports for all other scam types combined was $13,772. For job scam reports, average loss was 5.1% higher at $14,470.

[2] People who speak English as a second language are less likely to report scams than native speakers and are likely underrepresented in the data. When culturally and linguistically diverse community members do report to Scamwatch, they may choose not to identify English as their second language.

Figure 2: Job scam losses by age group (Scamwatch reports, 2024)

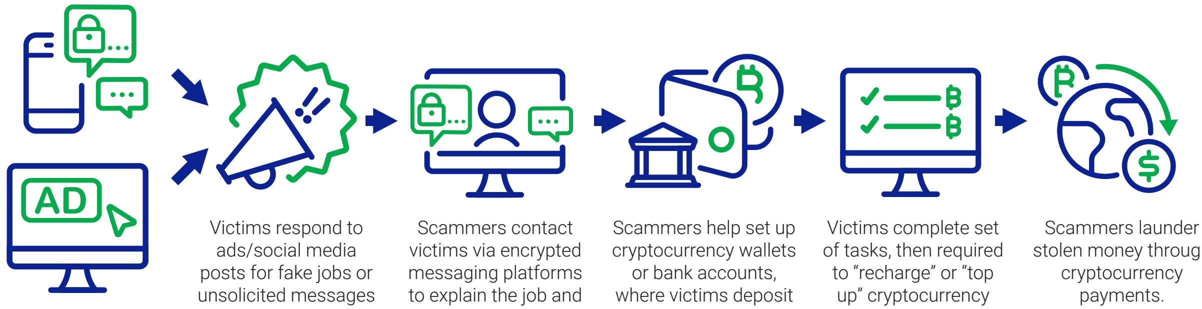


Three types of job scams were considered in scope for the Job Scam Fusion Cell:

- task-based job scams
- upfront fee payment job scams
- money mule job scams.

Task-based job scams

How a typical task-based job scam works



Scammers reach out to potential victims via texts or encrypted messages about an employment opportunity.

Scammers create ads/social media posts for fake jobs or impersonate recruitment agencies.

Victims respond to ads/social media posts for fake jobs or unsolicited messages from impersonated recruitment agencies.

Scammers contact victims via encrypted messaging platforms to explain the job and provide training.

Scammers help set up cryptocurrency wallets or bank accounts, where victims deposit money.

Victims complete set of tasks, then required to “recharge” or “top up” cryptocurrency to complete more tasks or receive a commission.

Scammers launder stolen money through cryptocurrency payments.

Task-based job scams deceive people into believing they are applying for a legitimate work-from-home opportunity with flexible hours. Scammers post fake job advertisements online or send unsolicited messages offering a job. These invitations often impersonate legitimate online jobs boards and recruitment agencies.

Once a person expresses interest in the job opportunity, the scammer will pose as a supervisor or mentor and establishes communication on an encrypted messaging app like WhatsApp or Telegram. The scammer will instruct the victim to set up a cryptocurrency account, providing step-by-step coaching where required, and direct the victim to create an account on a scam website.

Task-based job scam websites usually impersonate legitimate brands, such as Amazon, Instagram, or Myer. Victims believe they are working for the known brand and are given a set of simple, repetitive tasks to complete, such as buying or rating products and services. Tasks are usually required to be completed in sets or "packages" of 30 to 40 tasks per set.

After completing the first round of tasks, the victim may be paid a small amount of "commission." This may involve an actual transfer of cryptocurrency (usually the proceeds from previous scam victims), or the commission may simply appear to be credited to the victim's account on the scam website. This scam tactic is known as a "trust payment" and is used by scammers to convince victims that they are engaged in a legitimate job and that they will continue to receive earnings if they continue.

After completing additional tasks, the victim is required to "recharge" or "top up" their account to "unlock" new tasks or to access their earnings or commission. Victims are coached by the scammer to make payments to a cryptocurrency wallet or a bank account to complete the recharge.

Scammers assure their victim that they will receive back all the money they have paid, plus the commissions they've earned, once all the tasks are complete. However, the amount demanded by scammers to unlock tasks and commissions continues to increase until the victim stops making payments.

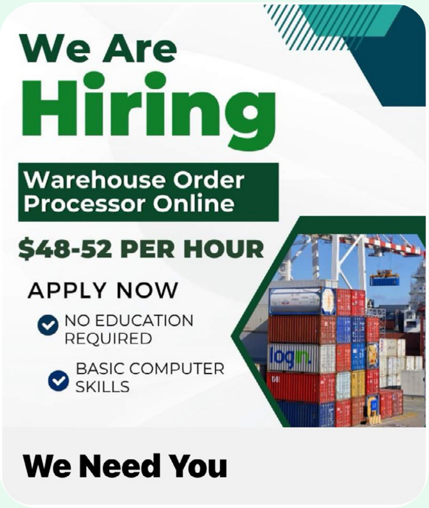
The criminals frequently coach their victims to borrow money from family and friends, to seek access to their superannuation, or to secure a bank loan in order to make the increasingly large payments. Scammers may also become aggressive if the victim stops making payments or questions the legitimacy of the job. Common tactics include using fake "letters of demand" or issuing legal threats to scare the victim into continuing to make payments.

Case study – Task-based job scam

Sophie found a job advertisement on Facebook, offering work as “Online Warehouse Processors.” The advertisement (pictured to the right) and accompanying description promised high rates of pay. Sophie provided her age, email address, and phone number. She received a WhatsApp message from a woman who identified herself as the “team leader,” who told Sophie that she would be working for a software company.

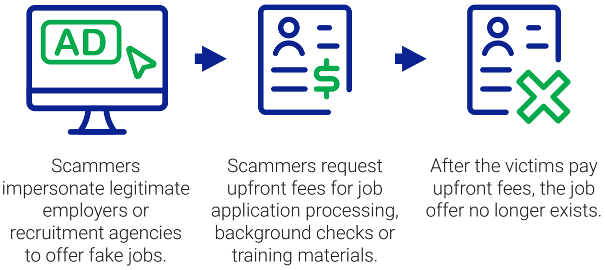
Sophie received training from the team leader and was shown how to create an account on a website pretending to be the legitimate software company. She was also instructed to open a cryptocurrency wallet. Sophie was told to complete sets of 40 orders, but in order to do so, she would need to top up her account with some of her own money, paid via cryptocurrency. Each set of tasks required a larger payment before she could complete it. Sophie did not have enough money to complete the tasks and was instructed to borrow funds from family and friends.

Sophie paid approximately $39,000 to the criminals while she completed the tasks. Once she stopped sending money, Sophie began receiving letters of demand, insisting she pay another $20,000 to receive her “investment” back.



Upfront fee job scams

How a typical upfront fee job scam works



Scammers impersonate legitimate employers or recruitment agencies to offer fake jobs.

Scammers request upfront fees for job application processing, background checks or training materials.

After the victims pay upfront fees, the job offer no longer exists.

Upfront fee job scams typically involve an element of impersonation, with scammers advertising a work opportunity on legitimate job websites or social media, and instructing victims to pay a fee before they can commence their employment. Impersonation of government agencies, education providers, migration agencies, and recruiters is common in upfront fee job scams.

The fees being demanded by scammers vary depending on the nature of the job being promised. Examples include fees for:

- training or qualification required for the role

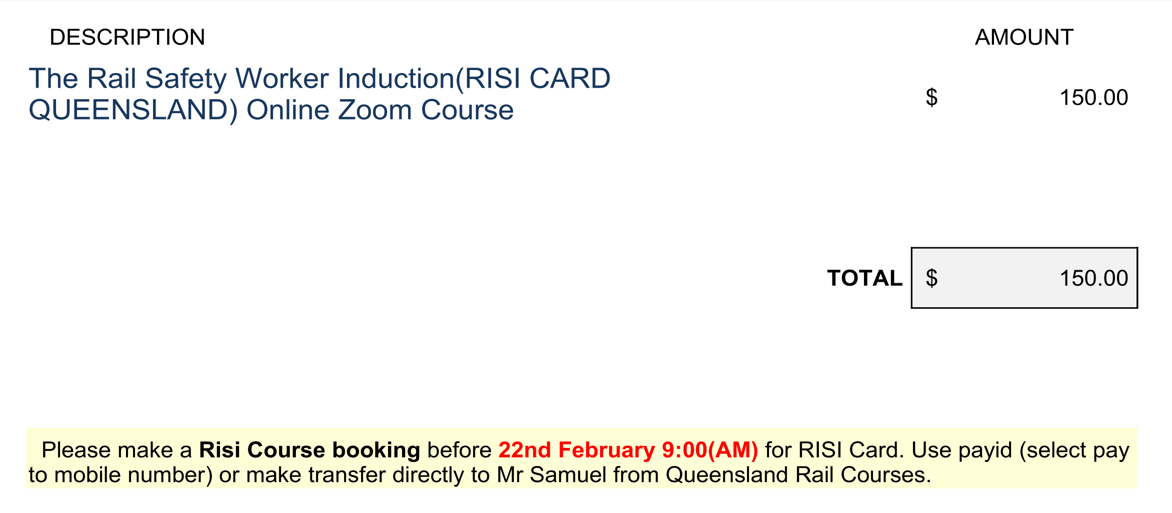
- visas to enter and work in Australia
- essential equipment (e.g. a computer and software) which must be purchased from the fake employer prior to starting work. Sometimes victims are directed to purchase through the fake employer's "nominated supplier" which is the same scammer (or group of scammers) operating under a different business name
- police check or other pre-employment checks
- mandatory uniform or other required equipment.

Once the victim pays the required fees, the scammer demands more money or breaks off communication with the victim. The victim faces the multiple impacts of financial loss, theft of personal information, and the non-existence of a job they believed they had secured.

Case study – Upfront fee job scam

Matt received an email about a job opportunity in a warehouse near his home. Matt emailed the recruiter and discussed the position. Matt researched the company online and believed that it looked like a legitimate company. As a result, Matt contacted the recruiter and accepted the job offer.

The recruiter advised that a Rail Industry Safety Induction was required to work in the warehouse, and as Matt wasn't already certified, asked him to pay $150 to register for the course. The recruiter later advised that the fee was incorrect and an additional $65.50 was required to secure a spot. Matt paid the extra fee but then received no further information about the warehouse position, even after following up multiple times.

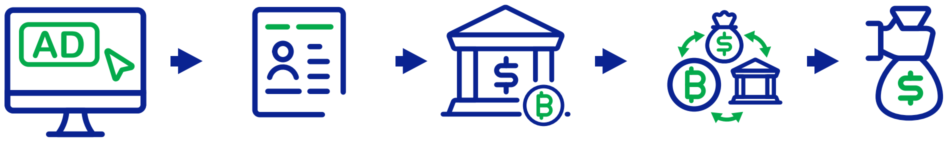


DESCRIPTION		AMOUNT
The Rail Safety Worker Induction(RISI CARD QUEENSLAND) Online Zoom Course		$ 150.00
	TOTAL	$ 150.00

Please make a **Risi Course booking** before **22nd February 9:00(AM)** for RISI Card. Use payid (select pay to mobile number) or make transfer directly to Mr Samuel from Queensland Rail Courses.

Money mule job scams

How a typical money mule job scam works



Scammers offer fake jobs on social media, messaging platforms, online pop-up ads, and emails.

The jobs often have titles like 'administrator', 'assistant', 'finance agent', 'remote cashier', or 'bookkeeper'.

The job requires victims to open a bank account or cryptocurrency account.

Victims receive money from scammers and asked to transfer money into other bank accounts and cryptocurrency accounts.

Victims receive a commission when transferring the money, as payment for their service.

Money mule job scams involve scammers recruiting victims to launder money that has been stolen and/or is used to fund serious crime. Money mule job scam victims are involved in criminal activity when moving stolen money between accounts. Intelligence from fusion cell participants indicates that some victims are aware or suspect that they've become involved in criminal activity, while others are genuinely unaware.

The roles advertised for this scam type typically include a financial element, such as "finance agent," "remote cashier," or "bookkeeper." Criminals advertise these roles on social media and messaging platforms, legitimate job board websites, through pop-up ads on websites, or via unsolicited emails.

Job seekers who apply for these roles may be directed to create additional personal bank accounts or they may be told to use their existing accounts. The scammer transfers money to the new "recruit" and provides instructions regarding where the money should be sent next. This destination may be a bank account or cryptocurrency wallet under the control of the scammer or their criminal associates, or the victim may be instructed to purchase gift cards and provide the details to the scammer. Sometimes the victim receives a commission when transferring the money as payment for their services.

To combat money mule scams, the Australian Federal Police (AFP) ran a campaign in 2024 and 2025 aimed at raising awareness of the scam type among international students. Because of this repeated attention from the AFP, the Job Scam Fusion Cell has had only a moderate focus on this type of job scam.

Case study – Money mule job scam

Tanya received an email about a job opportunity working as an administrator for a financial company. As the position offered the opportunity to work from home and fitted with her other commitments, Tanya accepted the offer.

She was provided with an "employment contract" which referred to her role as a "Billing Agent" and that she would be required to receive payments and transfer them to other accounts. The contract warned that a failure to on-forward payments in a reasonable time, would constitute a breach of contract, and enforcement action would be taken under Australian law.

Tanya was instructed to open 2 bank accounts in her own name, as well as an account on Kraken, the cryptocurrency trading platform. Tanya started receiving deposits into one of her newly opened bank accounts and was instructed to transfer those deposits to her other new bank account. She was then directed to transfer most of the money to her Kraken account, leaving a small amount behind as her "commission."

It wasn't until Tanya was contacted by her bank that she found out the job was a scam, and that the money she was transferring had been stolen from other scam victims. Tanya felt guilty and distressed at her involvement in the scam. Having provided significant amounts of personal information to the criminals involved, she is worried about the likely ongoing consequences.

Understanding victims' experiences

Fusion cell participants were committed to developing a deeper understanding of the experiences of job scam victims. By analysing intelligence reports and victim case studies, it was possible to identify common experiences, motivations, and decision-making patterns that influence engagement with scams. Fusion cell participants Myer and ANZ provided significant intelligence on victims' experiences; Myer from victims' reports to it as a business frequently impersonated in job scams, and ANZ from identifying job scam payments by unknowing customers.

The National Anti-Scam Centre conducted in-depth analysis of existing case studies and reports, and commissioned an academic review of job scam victimology, incorporating insights from both Australian and international sources.

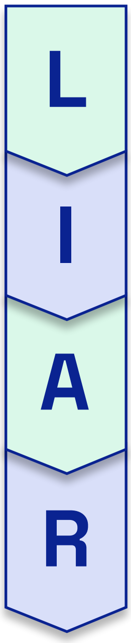
Job scams from an international perspective – academic review

To better understand victims' experience, the National Anti-Scam Centre commissioned fusion cell participant, Queensland University of Technology to undertake an academic review of job scam victim research, drawing insights from both Australian and international sources.

The review found that job scams are a significant crime type around the world, with victims in various jurisdictions reporting similar experiences. However, support services remain limited, making recovery of stolen funds difficult. Existing education and awareness efforts largely place the burden on individuals to detect scams rather than addressing the broader systemic issues.

Some international models, such as job hubs in Indonesia, take a strengths-based approach to prevention by upskilling job seekers and creating legitimate employment pathways. However, the universal need for work leaves individuals vulnerable, and there remain limited coordinated efforts to reduce this risk. Fusion cell participants discussed how to apply these findings to ongoing prevention and awareness efforts for job scams and the broader scam ecosystem, ensuring progress continues beyond the fusion cell's term.

A typical victim's journey in a task-based job scam can be summarised as:



Luring
Victims encounter fake job ads, unsolicited messages, or social media posts offering work. Many victims not actively looking for work engage, believing they've found a legitimate high-paying, flexible job opportunity. Once victims respond, scammers move their communications to an encrypted messaging platform like WhatsApp, Telegram, or iMessage.

Induction
Victims are added to encrypted messaging groups with "supervisors" and other "employees". The structured on-boarding, smooth communication, and success stories shared in these groups make it feel real. However, the "employees" are almost all scammers or bots.

Activity
The assigned tasks initially feel easy and earnings grow. The group chats use gamification techniques like leaderboards and bonuses to encourage participation. Completing more tasks unlocks higher rewards, reinforcing the sense of progress. Small "trust payments" are used to boost confidence. Victims are repeatedly required to pay money or cryptocurrency to complete sets of tasks or to earn commissions.

Realisation
Victims realise the scam when they cannot access their earnings. The "sunk cost" fallacy makes it difficult to justify quitting. Some victims are alerted to the scam by family or friends and give up, abandoning their losses, but many remain in the scam for longer periods (e.g. many months) hoping to recover their losses.

A victim's journey in a money mule job scam shares some similarities with a task-based job scam, victims are recruited into the scam typically by the same means and methods. Scammers often provide an "employment contract" or similar document to the victim to provide an appearance of legitimacy. This frequently has the added effect of causing the victim to believe any failure to follow the scammer's instructions will result in legal action. Victims may realise that they have been recruited to be a money mule when they are instructed to transfer money through their own account, however, many victims only become aware of the scam if their bank blocks payments or freezes their account.

A victim's journey in an upfront fee scam is often short, with the victim believing they are applying for a legitimate job opportunity and making a small (relative to the payments typically made in task-based job scams) upfront payment for legitimate-sounding purposes. Victims often realise they have been involved in a scam after they have made the payment, when they are unable to contact the scammer again.

Understanding these stages and the demographics of job scam victims has been critical in shaping the prevention strategies and awareness campaigns developed by the Job Scam Fusion Cell.

Awareness and prevention

As a learning from the Investment Scam Fusion Cell, the National Anti-Scam Centre developed an engagement and communications strategy to support the work of the Job Scam Fusion Cell. The strategy was designed to uplift communication with key stakeholders throughout the term of the fusion cell and to share results, learnings, and achievements following its completion.

The engagement and communications strategy aimed to:

- increase public awareness of job scams to empower identification, avoidance, and reporting, leading to a reduction in losses of money and personal information
- increase public understanding of the fusion cell as a key disruption initiative in the Government's anti-scam strategy and increase public confidence that businesses and government entities are collaborating to address scams
- provide greater recognition and understanding of the positive outcomes and benefits the National Anti-Scam Centre's fusion cells deliver in the fight against scams
- enhance effective communication between the National Anti-Scam Centre, fusion cell participants, stakeholders, other interested parties, and the Australian public.

During the first half of the fusion cell's term, the National Anti-Scam Centre engaged with members of industry sectors often impersonated by job scammers to raise awareness, implement preventative measures, and protect consumers. For example, best practice awareness messaging and prevention advice was provided to overseas-based staff of the Department of Home Affairs and the Department of Foreign Affairs and Trade, among others, to limit the ability of scammers to impersonate these senior departmental figures in job scams.

Another example relates to the healthcare sector. Fusion cell intelligence identified that healthcare providers were often impersonated by criminals in job advertisements in order to steal money and personal information from job seekers. Throughout its term, the National Anti-Scam Centre engaged with over 40 organisations in the sector, including industry bodies, organisations that were repeatedly impersonated, and state and territory government hospitals and health services, providing up-to-date advice on job scam trends, information on techniques used in the impersonation of healthcare organisations, and recommended awareness messaging for job seekers. Some health services engaged further with the National Anti-Scam Centre, receiving tailored advice regarding how to minimise the risk of impersonation of their organisation and how to protect potential job applicants.

These interventions appear to have had a substantial impact on scammers' attempts to target consumers seeking jobs in the Australian healthcare sector. As of late March 2025, there had been a near elimination of Scamwatch reports referencing job scams impersonating organisations in the sector.

The National Anti-Scam Centre also identified a cohort of external stakeholders with an interest in the work of the fusion cell. These organisations included Australian Government agencies such as the Australian Taxation Office and the Australian Securities and Investments Commission, digital platforms such as Apple, recruitment companies including Willo Talent, and organisations supporting international students and culturally and linguistically diverse communities.

Regular updates on the work of the fusion cell were shared with these stakeholders, as well as awareness messaging, fusion cell learnings, and intelligence for action where appropriate. Stakeholders also provided data and intelligence back to the National Anti-Scam Centre. As a result of this data sharing, some stakeholders are now in the process of being onboarded to the National Anti-Scam Centre's partner portal to facilitate expanded data sharing.

Job scams social media campaign

As a result of fusion cell research and intelligence, the National Anti-Scam Centre developed 2 targeted social media campaigns to raise awareness among cohorts at highest risk of job scams.

The *"How to spot and avoid job scams"* scam alert was released at the midway point of the fusion cell and was accompanied by organic social media posts. With high consumer engagement and re-sharing by fusion cell participants and stakeholders, this was at the time, the most viewed content on the Scamwatch Instagram channel.

A larger social media campaign was launched in early 2025. It incorporated both organic and paid content, and reflected a concerted effort to achieve stakeholder amplification of the messaging.

The organic component of the campaign was timed to coincide with university orientation in mid-February 2025. The National Anti-Scam Centre shared job scam awareness messaging across multiple channels, making use of image, carousel, and video posts. Fusion cell participants and other organisations were provided with social media collateral and key messages to share on their own channels, resulting in significant amplification of the messaging across social media, websites, and industry newsletters.[3]

The organic campaign was very successful, with a combined reach of over 66,000 unique users, and significant levels of engagement on Facebook where the ACCC has a large number of followers.

The National Anti-Scam Centre also ran a paid campaign on social media from 4–18 March 2025, using demographic-specific targeting to raise awareness among 2 at-risk groups; students and carers. The campaign achieved great results, with over 3.5 million impressions on Meta platforms, an increase of 1,000,000 impressions on the anticipated and benchmarked results.

Don't pay money to make money
If you're asked to pay money or cryptocurrency, it's a job scam.

Example of social media content posted in February 2025

[3] Stakeholders who shared content include the National Cyber Security Coordinator, Willo Talent, Crimestoppers NSW, Bankstown Police Area Command, Hays Australia, Study Tas, Study NT, Flinders University, RMIT University, Greenwich College, Australian Communications Consumer Action Network, Consumer Action Law Centre, Office of Fair Trading Queensland, NSW Fair Trading, The National Debt Helpline, and numerous Neighbourhood Watch groups, Facebook community groups, private investigators, and Facebook employment groups.

Figure 3: Engagement statistics from the Job Scam Fusion Cell social media campaign

Organic Campaign

479+ Likes and reactions

89k+ Reach

360+ Shares

Promoted Campaign

2.3M+ Total impressions

594 Meta clicks

927 Snapchat swipe ups

Tertiary education sector engagement

Intelligence from Scamwatch reports and fusion cell participants revealed that university students, and in particular international students, were being targeted by scammers, including through fake job advertisements being posted on university in-house job boards.

Due to the disproportionate harm experienced by scam victims in this cohort, the National Anti-Scam Centre developed a program of engagement with the tertiary education sector.

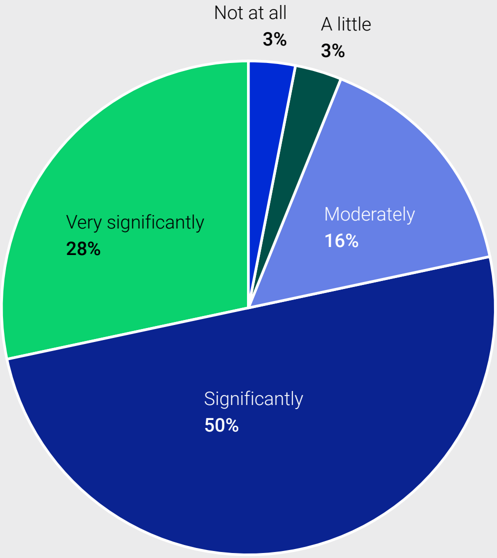
Universities and other institutions were notified of the rise in university job boards being targeted, and the risk of harm to their students. As a result, a number of institutions engaged with the National Anti-Scam Centre to seek advice on how to monitor for job scams on their online platforms and protect students.

In early March 2025, the National Anti-Scam Centre was invited to participate in Flinders University’s International Students Welcome Day to raise awareness on job scams impacting this cohort. In addition to the hundreds of copies of The Little Book of Scams in languages other than English given out prior to the event, over 250 students collected English language copies of The Little Book of Scams on the day, while many more watched videos produced by the National Anti-Scam Centre, scanned the QR code to download resources in their first language, and engaged with staff regarding how to stay safe from scams.

On 4 March 2025, the National Anti-Scam Centre hosted an online forum on job scams for the tertiary education sector. 130 people registered for the event, with 33 more joining on the day. Over 68 organisations were represented, including nearly every Australian university, TAFEs, English language schools, colleges, accommodation providers, and state and territory support hubs for international students. Fusion cell participants Adecco and the Australian Federal Police presented at the forum, respectively sharing best practice for reducing scams on university jobs boards, and awareness messaging regarding money muling among students. 75% of participants reported that their ability to identify and respond to job scams increased “significantly” or “very significantly” as a result of the event.

Job scams awareness at Flinders University's International Students Welcome Day in March 2025

As a result of the forum, my ability to identify and respond to job scams has increased:



Response to online questionnaire following tertiary education sector forum

The National Anti-Scam Centre continues to support organisations seeking to protect students, with "train the trainer" workshops being delivered to universities and state and territory international student support hubs. This training will assist organisations to deliver prevention and awareness messaging at key times throughout the year, ensuring that the learnings of the Job Scam Fusion Cell continue to assist this at-risk cohort in the months and years ahead.

Disruption activities and outcomes

Developing proof-of-concept disruption processes that extend beyond the term of the fusion cell is a key element of the fusion cell model. Disruption activities focused on the use of enabling technology, products, and services.

The National Anti-Scam Centre has built technology to support data sharing partnerships with stakeholders and has begun working with Job Scam Fusion Cell participants to bring them onto the National Anti-Scam Centre's information-sharing platforms.

Sharing scams data enables increased visibility of scam activity across government, law enforcement, and the private sector, providing organisations with better capability to identify and disrupt scams.

Table 1 Summary of removal requests – 8 Oct 2024 – 10 April 2025

	All platforms*	Website	Email	WhatsApp	Online job boards
Total referrals	1850	935	12	737	26
Successful	831	768	2	36	24
Unsuccessful[4]	414	141	8	264	0
Unknown result	605	26	2	437	2
% Success	45%	82%	17%	5%	92%

*Note that the "All platforms" category includes other referrals, for example bank accounts, iMessage, social media advertisements and profiles.

Confirmed rates of removal are low for most types of platforms, although actual rates of removal are much higher. The National Anti-Scam Centre does not consistently receive feedback on the outcomes of removal requests, except regarding websites and email addresses. Feedback from WhatsApp has varied over the term of the fusion cell, but the National Anti-Scam Centre generally does not receive feedback on the outcomes of individual removal requests. Some manual verification of the outcomes of removal requests is conducted, but this is very limited due to the resource-intensive nature of this work. A technological solution has been developed by the National Anti-Scam Centre to verify the outcomes of website removal requests without significant manual effort. While scam job advertisements on legitimate online jobs boards were relatively few in number, National Anti-Scam Centre engagement with these businesses and accessible reporting processes saw scam advertisements removed effectively.

[4] Removal requests deemed "unsuccessful" include scam enablers already removed by other methods and those requests where service providers were unable to prove scam activity and take action.

Payment disruption

Problem

Most job scams involve an attempt to obtain financial payment from victims. This may involve the victim transferring funds from their bank account directly to the scammer's account, or the payment may be made through other channels such as cryptocurrency. Cryptocurrency transactions are very common in task-based job scams and allow large amounts of funds to be quickly sent to recipients anywhere in the world. Recipients are generally very difficult to identify, and due to the anonymous nature of the blockchain, cryptocurrency transfers are almost always impossible to reverse.

Scammers often instruct victims to create an account with a digital currency exchange and to send funds from their bank account to the exchange, where the funds are converted into cryptocurrency and transferred to the scammer.

The fusion cell identified that scammers are responsive to measures intended to stop or add friction to scam payments. If banks limit transactions to identified high risk digital currency exchanges, for example, scammers quickly adapt their methods and instruct victims to send funds to other banks with less strict controls.

Opportunities

Many victims who report to Scamwatch, IDCARE, and ReportCyber provide details of the scammer cryptocurrency wallet addresses that they sent funds to. Fusion cell intelligence revealed that the same wallet addresses are often used to steal from multiple scam victims.

Where a digital currency exchange is involved in a scam transaction, the process could be disrupted by either the victim's bank, or the exchange.

The fusion cell identified the likelihood of patterns in transactions associated with task-based and money mule job scams. Larger banks and reputable digital currency exchanges, such as those participating in the Job Scam Fusion Cell, have highly sophisticated systems in place to detect and analyse such patterns, but many smaller financial institutions have far less capability.

Actions

In collaboration with the Joint Policing Cybercrime Coordination Centre (JPC3) and AUSTRAC, the National Anti-Scam Centre commenced a trial to share cryptocurrency addresses that have been included in job scam reports to Scamwatch and IDCARE. Since January 2025, the National Anti-Scam Centre has shared over 800 wallet addresses with 6 digital currency exchanges as part of this trial. These exchanges account for around 80% of Australian cryptocurrency transactions. The referral does not imply an allegation of criminality, but is an indicator of heightened risk, and the exchanges perform their own investigation into the use of the wallet.

Cryptocurrency wallet addresses were also shared directly with the digital currency exchanges participating in the fusion cell, enabling them to conduct investigations and analysis.

The National Anti-Scam Centre also shared bank account details of suspected mule accounts with banks where appropriate, for investigation and action. In addition, a payment tracing trial was conducted, with significant effort from Commonwealth Bank and Crypto.com, to determine payment patterns and exit points for conversion of scam cryptocurrency payments into fiat.

Fusion cell participants completed a survey to identify key risk indicators associated with job scams. Data gathered in the survey included typical payment amounts, payment patterns, and customer characteristics. The fusion cell then developed a guide based on this intelligence to assist smaller banks, credit unions, and digital currency exchanges in detecting and disrupting job scams.

Outcomes

The sharing of job scam cryptocurrency wallet addresses collected through Scamwatch reports and from fusion cell participants led to investigation and analysis by participating digital currency exchanges. Both Swyftx and Crypto.com assisted in identifying suspicious transactions related to external wallet addresses collected and shared by the National Anti-Scam Centre. The exchanges proactively blacklisted the wallets and shared the information with other platforms, helping to amplify the blocking of confirmed scam wallets across the ecosystem. In one referral tranche of suspicious wallets from the National Anti-Scam Centre, Crypto.com determined that 65% of customers associated with the scammer wallets were not already identified as being linked to scam activity.

The sharing of cryptocurrency addresses has provided a valuable proof-of-concept trial for collating and sharing suspect cryptocurrency wallets. The National Anti-Scam Centre is looking to expand and automate sharing of scammer wallet addresses from stakeholders in the future, ensuring the work of the fusion cell is able to continue to have an impact long beyond its 6 month term.

The fusion cell produced a *Guide to Disrupting Job Scam Payments*. It offers businesses in the banking, payments, and cryptocurrency sectors practical advice based on the best practices of industry leaders. It includes risk indicators, scripts and examples of warning messaging, and questions for staff to ask customers identified as potential job scam victims. This resource will persist beyond the fusion cell and continue to help businesses disrupt job scam payments in the future.

Website disruption

Problem

Criminals use scam websites to deceive their victims and to create the illusion of a legitimate employment opportunity. Links to scam websites can be found on search engines and social media platforms, and displayed as advertisements alongside trusted content.

Scammers often infringe the intellectual property rights of well-known businesses, by using their logos, branding website design and copyright material, to give scam websites the appearance of legitimacy. Multiple identical or nearly identical websites may be created[5], so that if one website is taken down, the scammer can simply direct victims to another site. In many cases, only a single character will distinguish a fake URL from the legitimate one, for example, a hyphen inserted between words or a numeral “1” in place of a capital letter “i”.

As well as harming scam victims, the websites can have significant financial, reputational and legal impacts on the businesses impersonated. While high profile companies are often impersonated, many small and medium sized Australian businesses also find themselves impersonated online in scammers’ attempts to steal from consumers.

In task-based job scams, scam websites are the platform to which victims are directed to complete their tasks, and it’s on these sites that victims see their “earnings” and “balance” increase and decrease.

[5] Often 10 or more websites are created by scammers at a time.

Opportunities

Removing or blocking scam websites is an essential element of protecting consumers from job scams; the longer a website remains active, the greater the number of consumers who may encounter it. Websites that have been active for a long time have a greater appearance of legitimacy. While scammers can easily re-establish a scam site using a different URL, the very limited history of the new site will be identified as a reason for caution by some consumers and user protection systems.

Disruption of job scam websites reduces scammers' ability to run the task elements of the scam, which limits the funds they can steal from victims. Disruption of websites also reduces opportunities for scammers to gather contact details, identity documents and other personal information which can be used to perpetrate future scams.

In addition, victims of job scams may realise they are involved in a scam if the website is taken down. Job scam reporters to Scamwatch described that seeing a website was no longer active provided their first warning of the scam and prevented them from sending money to the criminals behind it (see "Case study – Website removals making a difference," below).

Actions

The National Anti-Scam Centre built upon the work on the Investment Scam Fusion Cell to disrupt scams by removing and blocking scam websites. All Scamwatch reports of job scams were reviewed and analysed daily, with scam website URLs referred for blocking or removal. Intelligence from fusion cell participants and other organisations in Australia and overseas was also used to identify job scam websites.

It is essential that legitimate organisations have confidence in the processes of the National Anti-Scam Centre, and that the risk of a legitimate website being removed is mitigated. The National Anti-Scam Centre regularly contacted businesses impersonated by job scam websites to seek confirmation that they were not operating the scam websites. In addition, the National Anti-Scam Centre recommended these organisations continue to take their own action to protect their customers, reputation and intellectual property, and provided further advice and best practice awareness messaging.

High priority disruption work during the term of the fusion cell included action to counter the impersonation of Australian Government entities, including the Department of Foreign Affairs and Trade, the Department of Home Affairs, APSJobs.gov.au, and approved employers in the Pacific Australia Labour Mobility (PALM scheme). As well as taking action to remove websites and blocking email addresses impersonating these entities, the National Anti-Scam Centre provided best practice advice (including to overseas-based frontline staff) to uplift scams awareness and protection.

The National Anti-Scam Centre implemented an immediate and high-level response when fusion cell intelligence indicated that persons holding Australian Government Security Vetting Agency security clearances were being targeted by job scammers. Intelligence suggested that the identified job advertisements revealed attempts to steal personal information. This compromised information was then likely to be used to access IT infrastructure and online systems. The National Anti-Scam Centre engaged with a range of job boards and other digital platforms in Australian and overseas, and took additional steps to notify relevant parties.

Outcomes

935 job scam websites were referred to the National Anti-Scam Centre's contracted scam website removal service during the 6 month term of the Job Scam Fusion Cell, and 768 had been removed at the time of writing this report. These websites were not being identified as illegitimate by other means and may otherwise have remained live and exposed more Australians to the risk of being scammed. Over 100 of the job scam websites removed were referred from state law enforcement agencies as part of a fusion cell proof-of-concept trial. This collaboration was highly successful, and the National Anti-Scam Centre is preparing to expand this work to include other scam types and other scam enablers, and to extend the collaboration beyond the term of the fusion cell.

The engagement with overseas-based job boards established by the fusion cell has contributed to the National Anti-Scam Centre being seen as a world leader in decisive disruption action against scams. Businesses based in other countries frequently contact the National Anti-Scam Centre to request advice, assistance, or best practice regarding impersonation, disruption and general scam safety. These businesses in the jobs and recruitment sector have begun referring contacts in other sectors, e.g. cyber-security, to the National Anti-Scam Centre for assistance understanding the relevant principles and other guidance.

Fusion cell participants identified and collated the data points needed by different service providers to disrupt job scams. The National Anti-Scam Centre developed a resource that aims to assist businesses impacted by impersonation scams to navigate platform-specific reporting requirements. The resource provides advice for submitting requests to service providers, outlines the required data points and evidence, and provides contact points and escalation pathways. Feedback from fusion cell participants has improved disruption outcomes and has been incorporated into the National Anti-Scam Centre's disruption processes.

Through the Job Scam Fusion Cell, the National Anti-Scam Centre's existing removal capabilities have been expanded by onboarding to the TikTok and LinkedIn takedown portals, enabling direct requests for content removal. This enhanced capability for scam disruption will remain beyond the conclusion of the fusion cell.

As a result of this disruption work, the National Anti-Scam Centre is developing automated processes to support the verification of organisations being impersonated by scammers and the subsequent disruption of scam enablers. It is anticipated that this will initially support the disruption of job scams and high loss imposter bond scams, with further expansion to follow.

Case study – Website removals making a difference

An example of the positive impact of the Job Scam Fusion Cell can be seen in the case of a scam impersonating ADL Accounting, a website-enabled task-based job scam. Based on fusion cell intelligence, a request for removal of the website was made on 28 October 2024, and the site was taken offline in the early hours of 29 October 2024.

Later on 29 October, a job scam victim who had been involved in the scam returned to the site. When noticing that the site was offline, they were alerted to the scam, before they had sent any money to the scammers.

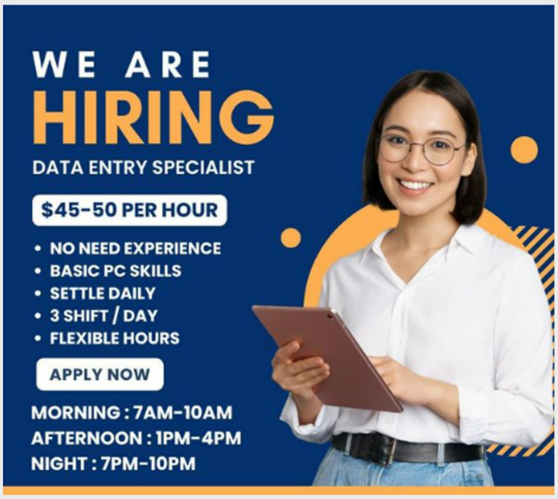
The National Anti-Scam Centre subsequently determined that this scam had been operating from the same website for over a year and had been targeting victims in the United States during that time.

Job scam advertisement disruption

Problem

Criminals use a range of advertising methods to make contact with potential victims. Job scam advertisements are primarily found on social media platforms, search engines, and on legitimate job and employment websites.

Job scam advertisements are challenging to monitor and disrupt because they can be difficult to distinguish from legitimate job advertisements. Scammers use generic language and images in advertisements to avoid detection and they typically offer remote flexible work opportunities. Advertisements promise short daily hours and high rates of pay, with no experience needed.



Job scam advertisement from social media

Opportunities

The National Anti-Scam Centre analysed job scam advertisements reported to it via the Scamwatch website and proactively identified through open-source research. A range of indicators of job scam advertisements were identified, including language, job titles, design, next step instructions, conditions and more. Trends and patterns in advertisements over time were also considered.

The National Anti-Scam Centre also discussed scam monitoring techniques and disruption tactics with legitimate job website providers and recruitment agencies who were part of the fusion cell.

Actions

The National Anti-Scam Centre developed a keywords and trends intelligence product which is shared with stakeholders on a regular basis to assist with their job scam monitoring and disruption efforts. The National Anti-Scam Centre also engaged closely with fusion cell participants to identify the types of information that are most valuable to them in disrupting job scam advertisements.

Fusion cell participant SEEK provided intelligence and insights into data points and processes for identifying high risk advertisers and advertisements, which shaped National Anti-Scam Centre advice to recruiters, universities and other organisations.

Outcomes

The keywords and trends intelligence product has become a source of information and guidance for digital platforms, and organisations in the recruitment and advertising sectors, including some which were not part of the fusion cell. The intelligence product supports businesses to uplift their scams resilience and protection for Australian consumers who use these platforms.

The keyword and trends intelligence product is now being expanded to include other scam types, and work is underway to automate the processes of gathering and sharing this intelligence.

Stakeholder perspective – Meta[6]

Meta's ongoing partnership with the National Anti-Scam Centre and the Job Scam Fusion Cell demonstrates the power of collaboration between government, industry, and organisations in combating scams. Through our intelligence-sharing efforts, we have successfully removed approximately 29,000 accounts engaged in job scams in Australian Facebook groups. The timely exchange of valuable insights from the National Anti-Scam Centre has been instrumental in enhancing our systems, driving product improvements, and strengthening detection and enforcement measures to safeguard not only Australians but all our users worldwide.

In addition to removing accounts engaged in job scams, over the same time period we increased our enforcement on accounts targeting Australian users originating from criminal scam centres. This includes approximately 77,000 users and 17,000 ads. Disabled scam accounts made a total of 840,000 posts in Australian Facebook Groups during this time, demonstrating the importance of this work.

Encrypted and unsolicited message disruption

Problem

Scammers frequently use encrypted messaging apps, such as WhatsApp, iMessage or Telegram, to make the initial, unsolicited, contact with their victim. These messages frequently impersonate a legitimate recruitment agency or jobs board website. Where the initial contact is via a social media post or some other means, the scammer generally directs their victim to an encrypted messaging platform for ongoing communication.

Providers of encrypted messaging services have no visibility of message content and are therefore reluctant to block services based solely on evidence from a screenshot or an external scam report, due to the possibility that these may be false or doctored.

Opportunities

Popular encrypted messaging apps allow users to report scam content in-app. For example, if a person receives a scam message on WhatsApp, the recipient can report the chat or report a single message. Reporting a chat sends the 5 most recent messages, unencrypted, to the WhatsApp Trust & Safety Team for review. Reporting a single message does the same with the selected message. WhatsApp is then able to take action, by blocking accounts being operated by scammers. The Scamwatch form asks reporters if they have reported the scam anywhere else, providing a drop-down list and a free text field for a response. From a 30-day sample of Scamwatch job scam

[6] Content in this information box provided by Meta.

reports, where the victim lost money and was contacted via WhatsApp (70 reports), not a single victim indicated that they had reported the scam messages to WhatsApp.

Telegram and Signal appear in scam reports much less frequently and both provide the means to report messages in-app. Notably, reporting a Signal message appears to be aimed at reducing automated spam, not scams. Reporting in the Signal app does not send unencrypted content for investigation. Rather, if multiple reports are received, the sender will be required to supply "proof of humanity" to continue using the service.[7]

Actions

The National Anti-Scam Centre has developed public messaging encouraging Australians to report in-app if they receive job scam messages on an encrypted messaging platform. This important message was shared widely for the first time via the job scams social media campaign which was launched in March 2025. This content will continue to be shared regularly on social media after the fusion cell concludes.

The National Anti-Scam Centre has also been working with jobs board websites and organisations in frequently impersonated sectors, such as healthcare, to inform them of the risk of impersonation in scams and to provide example awareness messaging.

The Scamwatch reporting form provides an opportunity for reporters to specify the scammer's initial method of contact. The National Anti-Scam Centre is developing tailored auto-response emails to be sent when a reporter identifies an encrypted messaging service as the initial contact method. This email will ask the reporter to also report their concerns in-app, and provide instructions for doing so.

The National Anti-Scam Centre is developing systems to ensure that scammer details sourced through activities unique to the fusion cell can be processed for disruption alongside details obtained from Scamwatch reports. For example, Calling Line Identifiers (CLIs, e.g. phone numbers) verified as scam enablers by fusion cell participants are referred to telecommunication providers for investigation and disruption in parallel with unverified CLIs from Scamwatch reports.

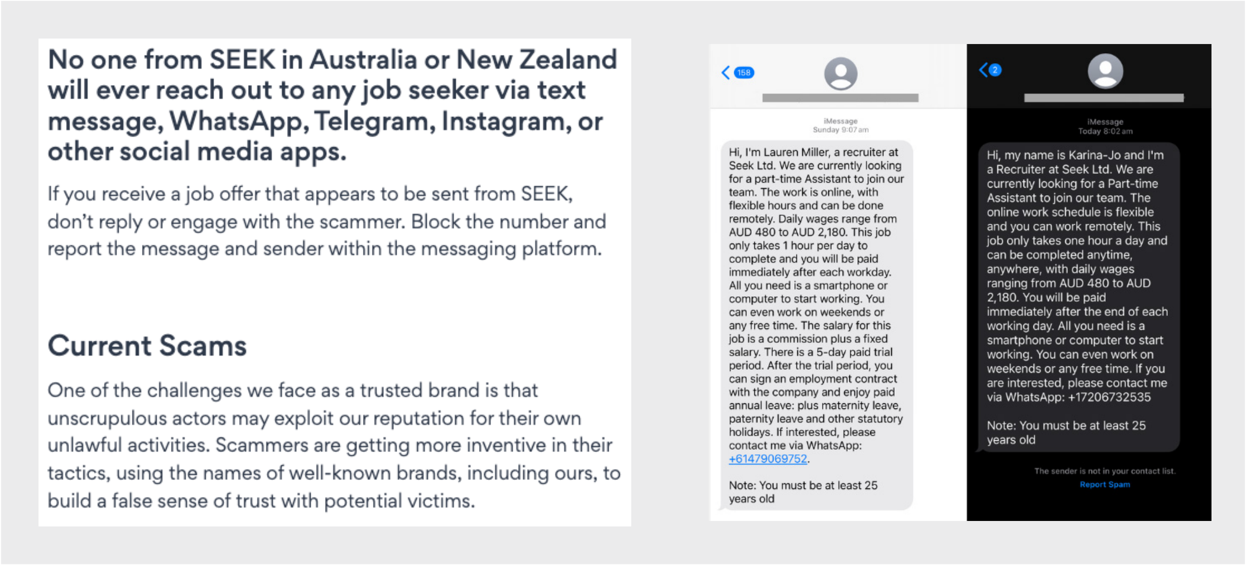
Outcomes

The National Anti-Scam Centre's engagement with frequently impersonated entities, such as jobs boards, noted above has led to an observable increase in awareness raising messaging by these businesses. Using messaging templates supplied by the National Anti-Scam Centre, businesses are alerting consumers to the likelihood of impersonation, notifying them of legitimate communication methods, and providing means of verifying contact that appears to come from the business.

In late February 2025, fusion cell participant SEEK updated its "Security and Privacy Hub" with the fusion cell recommended messaging and added examples of SEEK being impersonated in job ads to other scam examples on its website. Only days later, on 6 March, a consumer received a text message impersonating SEEK and offering flexible, highly paid work. On visiting the SEEK website, the consumer saw the warning message alerting them to the scam and the posted example of the text message identical to the one they had received. The consumer then reported the scam attempt to Scamwatch.

[7] https://signal.org/blog/keeping-spam-off-signal.

Example of SEEK messaging and smishing attempts



No one from SEEK in Australia or New Zealand will ever reach out to any job seeker via text message, WhatsApp, Telegram, Instagram, or other social media apps.

If you receive a job offer that appears to be sent from SEEK, don't reply or engage with the scammer. Block the number and report the message and sender within the messaging platform.

Current Scams

One of the challenges we face as a trusted brand is that unscrupulous actors may exploit our reputation for their own unlawful activities. Scammers are getting more inventive in their tactics, using the names of well-known brands, including ours, to build a false sense of trust with potential victims.

[redacted]

iMessage
Sunday 9:07 am

Hi, I'm Lauren Miller, a recruiter at Seek Ltd. We are currently looking for a part-time Assistant to join our team. The work is online, with flexible hours and can be done remotely. Daily wages range from AUD 480 to AUD 2,180. This job only takes 1 hour per day to complete and you will be paid immediately after each workday. All you need is a smartphone or computer to start working. You can even work on weekends or any free time. The salary for this job is a commission plus a fixed salary. There is a 5-day paid trial period. After the trial period, you can sign an employment contract with the company and enjoy paid annual leave: plus maternity leave, paternity leave and other statutory holidays. If interested, please contact me via WhatsApp: +61479069752.

Note: You must be at least 25 years old

[redacted]

iMessage
Today 8:02 am

Hi, my name is Karina-Jo and I'm a Recruiter at Seek Ltd. We are currently looking for a Part-time Assistant to join our team. The online work schedule is flexible and you can work remotely. This job only takes one hour a day and can be completed anytime, anywhere, with daily wages ranging from AUD 480 to AUD 2,180. You will be paid immediately after the end of each working day. All you need is a smartphone or computer to start working. You can even work on weekends or any free time. If you are interested, please contact me via WhatsApp: +17206732535

Note: You must be at least 25 years old

The sender is not in your contact list.

Barriers to disruption

The objectives of the Job Scam Fusion Cell included identifying and reporting on barriers to coordinated scam prevention and disruption. The following potential barriers were identified during the course of the fusion cell. Steps taken or planned to mitigate these challenges are included below where appropriate.

Challenges in actioning disruption requests

- Fusion cell participants identified challenges in actioning some disruption requests, particularly the removal of accounts on encrypted messaging platforms, the disruption of suspected scam email addresses, and difficulties blocking phone numbers used in scams.
- Encryption of over-the-top messaging services means providers have no visibility of message content. Service providers are therefore reluctant to block accounts based solely on evidence from a screenshot or Scamwatch report, due to the possibility that the screenshot or report is false or doctored. The National Anti-Scam Centre has been working closely with stakeholders to map out their processes and required data points to ensure that future requests can be more easily actioned by the recipient.
- Similarly, service providers do not generally consider a screenshot or transcript of a scam email sufficient evidence of illegal activity to warrant blocking or removal of an email account. If email headers from scam emails are included in referrals to service providers, successful disruption outcomes are much more likely.[8] However, few email users are familiar with accessing headers and as such they are not often included in scam reports.
- The National Anti-Scam Centre refers phone numbers included in Scamwatch reports to telecommunications providers which in turn investigate and identify, trace, and block SMS scams. The volume of phone numbers used in SMS scams is extremely high, making blocking challenging. The Australian Communications and Media Authority is currently focused on rebuilding confidence in the use of telephone numbers and brands by developing new regulatory arrangements for use of SMS sender IDs, as well as establishing a new Telecommunications Numbering Plan.
- All of the digital platforms participating in the fusion cell have clear referral pathways or contact points for persons wishing to report a scammer using that platform. However, on many other platforms it is less clear how to report scam content. Reflecting its role as a coordinator of disruption efforts, and a desire to integrate existing efforts rather than duplicate them, the National Anti-Scam Centre has produced an Impersonation Response Toolkit for businesses. This guide provides instructions and contact details for removal of scam content on over 60 different platforms, including social media services, online marketplaces, financial institutions, and telecommunications services.
- The lack of responsiveness from some service providers regarding the status of requests for removal is also a barrier to effective disruption. Not knowing the success or otherwise of requests creates challenges for prioritisation and the allocation of resources. The National Anti-Scam Centre is working with stakeholders to develop efficient mechanisms to provide feedback on disruption requests. The cryptocurrency trial noted above has been specifically designed to include mechanisms for tracking the status of requests. In addition, a technological solution has been developed to automatically verify the status of some requests for website removal.

[8] Email headers are technical details included, though not usually visible, in an email message. The headers include information on the sender, the software used to compose the message, the email servers through which the message passed on its way to the recipient, and authentication results which verify if the message originated on the stated server.

Where the National Anti-Scam Centre receives disruption requests from other sources, providing feedback on their status and outcomes to the requesting organisations has been made a priority.

The need for effective, accessible data-sharing

- The National Anti-Scam Centre provides a central connection point for organisations to share data to combat scams and encourages organisations to consider the benefits of increasing the connections between data sources across the ecosystem.
- Fusion cells have demonstrated a significant opportunity to enhance data sharing and connections between data sharing platforms like the Australian Financial Crimes Exchange (AFCX) and the National Anti-Scam Centre. By connecting more organisations involved in anti-scam activities and enabling broader data sharing, disruption efforts can be implemented at scale. Recognising that some organisations share some data on different platforms, greater connection of these data sources will increase visibility of scam activity across the ecosystem and increase disruption opportunities.

The limitations of manual disruption processes

- As noted above, the fusion cell model creates a sandbox environment for proof-of-concept trials. However, for ongoing effect, beyond the term of the fusion cell, and to be scalable to include other scam types, disruption mechanisms must transition to automated processes. Without sustainable automated processes, once the fusion cell ends participants may turn their attention to other priorities and disruption processes may falter.
- Where disruption processes developed in the fusion cell proved to be effective and are likely to have ongoing value, the National Anti-Scam Centre is working to automate some or all elements of the processes. Many disruption activities are likely to require some manual review or verification. Consideration is therefore being given to how these steps can be integrated into existing National Anti-Scam Centre processes to minimise manual handling and reduce the time taken for disruption.

Scalability of website disruption

- Criminals engaged in job scams operate large numbers of websites to evade disruption. Stakeholders in the scam ecosystem frequently refer to the “whack-a-mole” effect, where a scam website is taken down, only to be replaced by another within minutes. Even if it was possible to remove every website reported to Scamwatch in close to real time, the large criminal networks behind many scams would suffer little impact. Effective disruption requires the ability to detect and remove websites at scale, including detection and removal prior to a victim encountering and reporting the site.
- Having observed the effectiveness of the keywords and trends intelligence product in the Job Scam Fusion Cell, the National Anti-Scam Centre is working to implement intelligence sharing with Meta and Google to proactively disrupt scam content at scale, and without relying on consumer reports regarding individual websites.

Different categorisation or mis-categorisation of scams

- Some stakeholders were (and continue to be) reluctant to commit resources to disrupting job scams because the scam type is considered insignificant in comparison to other, higher financial loss, types of scams. The nature of victim harm resulting from job scams (as described above) may not be well understood, including the fact that vulnerable cohorts within the community are disproportionately impacted by these types of scams. The reluctance of some stakeholders to commit resources to disruption is also likely due to different categorisation or mis-categorisation of job scams by stakeholders, which gives the appearance of much lower levels of job scam activity.

Looking forward

During the term of the Job Scam Fusion Cell, the *Scams Prevention Framework Act 2025* was passed by the Australian Parliament.[9] The Scams Prevention Framework (SPF) establishes world-leading protections against scams and creates enforceable obligations on entities in designated sectors.

Some participants of future fusion cells are likely to be operating in designated sectors under the SPF, and as such will be required to take reasonable steps to prevent and detect scams relating to, connected with, or using their regulated services, to have documented governance policies and procedures in place to combat scams, and to provide accessible reporting and dispute resolution procedures.

Fusion cells complement the SPF by enabling regulated and non-regulated entities to better understand scam issues and share information about how to combat them. Future fusion cells may also provide an opportunity to identify gaps in the scams ecosystem. Fusion cells also create opportunities for the ACCC and others to develop information-sharing processes with non-regulated entities (e.g. cryptocurrency firms).

It will be important that future fusion cells continue to encourage businesses to share information. There will be an ongoing need for voluntary information sharing in order to respond to rapidly evolving scams. Fusion cells provide an environment for identifying and exploring these opportunities.

Outside fusion cells, the National Anti-Scam Centre has been working with stakeholders to develop processes to assist them to effectively share scam intelligence with, and receive such intelligence from, the National Anti-Scam Centre. The Job Scam Fusion Cell has provided an opportunity to test some of these processes.

The Job Scam Fusion Cell has demonstrated the value of sharing scam intelligence, with the cryptocurrency wallet trial noted above being a clear example; Scam wallet data reported to Scamwatch by consumers was shared with digital currency exchanges, leading to the blacklisting of wallets on multiple exchanges. Conversely, as noted above, sharing intelligence to disrupt suspected scam email addresses, or scam content on encrypted messaging platforms has been very challenging to implement.

Learnings from the Job Scam Fusion Cell and potential future adjustments to address the challenges experienced, will be considered by the National Anti-Scam Centre and key stakeholders in planning for future fusion cells.

[9] ACCC welcomes passage of world-first scams prevention laws | ACCC.

Appendix A: 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 processes and reporters withdrawing reports. In addition, changes were made to the Scamwatch report form which have minor impacts on the data represented on the Scamwatch public statistics page and data in this report. For example, a new field for recording cryptocurrency losses was added in March 2024, and although there was some delay in this loss data being uploaded to the public statistics page, this report and other National Anti-Scam Centre publications now include that data.

While effort is made to verify high loss reports, some reports remain unverified. Scamwatch data is publicly available at https://www.scamwatch.gov.au/research-and-resources/scam-statistics.

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.

This report has been deliberately written so as not to disclose processes and other information that could assist criminals to counter scam prevention and disruption efforts.

Not all Australians report scams. Despite the existence of multiple reporting platforms, the extent and impact of scams is under-reported, and some cohorts are markedly under-represented in official reporting figures, as noted above.

The Australian Bureau of Statistics Personal Fraud data shows that in the 2022–23 financial year (the most recent data available), 2.5% of Australians (514,300) experienced a scam.[10] 69% of people who experienced a scam notified (or were notified by) an authority. This means that approximately 30% of people who experienced a scam did not report it. It is likely many of those who did not report the scam incurred a small or no direct financial loss. Consequently, this under-reporting does not mean actual losses would be 30% higher if those people had reported.

[10] Source: https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/latest-release accessed 7 February 2025.

Australian Government

National Anti-Scam Centre