Level 17, 2 Lonsdale Street
Melbourne Vic 3000

GPO Box 520
Melbourne Vic 3001

www.accc.gov.au

Contact Officer:
Contact Phone:

20 December 2023

Committee Secretary
Parliamentary Joint Committee on Law Enforcement
PO Box 6100
Parliament House
Canberra ACT 2600

By email: le.committee@aph.gov.au

Dear Committee Secretary,

Re: Inquiry into the capability of law enforcement to respond to cybercrime

I refer to the inquiry initiated by the Parliamentary Joint Committee on Law Enforcement (**PJCLE**) into the capability of law enforcement to respond to cybercrime (**inquiry**), as outlined in the terms of reference.

The Australian Competition and Consumer Commission (**ACCC**) is an independent Commonwealth statutory agency that promotes competition, fair trading, and product safety for the benefit of consumers, businesses, and the Australian community. The primary responsibilities of the ACCC are to enforce compliance with the competition, consumer protection, fair trading, and product safety provisions of the *Competition and Consumer Act 2010*, regulate national infrastructure, and undertake market studies.

The ACCC welcomes the opportunity to provide information to the current inquiry. The ACCC's response focusses on financial crimes known as scams, many of which are cyber-dependent or cyber-enabled. The ACCC acknowledges there is significant overlap between scams, fraud, and other types of cybercrime – some but not all scams involve cybercrime and some but not all cybercrime can be described as a scam. As such, a range of government agencies are already responding in this space, and it is important that government and agencies adopt a coordinated approach whilst drawing on the different strengths of each agency.

This submission addresses Terms of Reference 1, 3, 5 and 6, being those relevant to scam detection, investigation, and prosecution. The submission draws on the ACCC's experience running the Scamwatch service for over 16 years as well as our more recent experience following the establishment of the National Anti-Scam Centre. Scamwatch receives over 240,000 scam reports each year including reports from Australians who have been victims of cyber-dependent or cyber-enabled scams. So far in 2023, Scamwatch has received 280,244 reports with $455 million reported lost to scams. Of these, over 27,740 have reported direct financial loss, and overall, 76,116 have reported some type of financial or information loss.[1]

In 2023, the government allocated $58 million over 3 years to establish the National Anti-Scam Centre within the ACCC to make Australia a harder target for scammers. The National Anti-Scam Centre is focussing on three key capabilities:

[1] Scamwatch report data 1 January to 30 November 2023.

1. **Collecting and sharing data and intelligence** across the scam ecosystem to enable the early identification of scam trends. This intelligence, shared with law enforcement, government departments and agencies, consumer groups, and the private sector, will inform education and disruption efforts, focusing on early intervention to reduce or prevent losses to scams.
2. **Coordinating scams prevention, disruption, and awareness activities** by drawing on expertise across government, law enforcement, industry, and consumer organisations to lead a nationally coordinated, timely, anti-scam strategy.
3. **Helping consumers spot and avoid scams** by working with the National Anti-Scam Centre partners across the scams ecosystem to support consistent messaging and provide better education resources to help consumers protect themselves and others.

Through these capabilities, and by coordinating engagement across all states and territories, the National Anti-Scam Centre aims to support Australia's law enforcement agencies to detect and investigate scams and prosecute those responsible.

Recommendation 1: The introduction of innovative, agile, and automatic processes for tracing and freezing cryptocurrency assets to increase the capability of law enforcement agencies to investigate and prosecute cybercrime.

The ACCC recognises the need to increase capability and resources for Commonwealth and State law enforcement to investigate and prosecute cyber-enabled crime, including scams. Many scams are enabled by technology and the rapid increase in sophistication in recent years is leading to significant financial loss.

This year Australians have reported to Scamwatch losses of $158.3 million in scams where cryptocurrency is the payment method.[2] This represents a 12% increase compared to the same period in 2022. Cryptocurrency is a common payment method across a range of scams particularly investment scams, employment scams, and romance scams.

Law enforcement capability to act quickly to freeze, trace, and recover cryptocurrency is critical. Since many scams and cybercrimes involve multiple payments, often starting small and increasing in size, the ability to rapidly identify and freeze cryptocurrency wallets used for illegal activity would directly reduce financial losses.

The ACCC has a rich source of up-to-date intelligence on scams involving cybercrime through reports made to the Scamwatch service now managed within the National Anti-Scam Centre. The ACCC recognises other organisations also hold valuable data and information relating to scams and cybercrime. The ACCC is funded to provide IT infrastructure through the National Anti-Scam Centre to support high frequency data sharing with a range of government agencies, law enforcement, and the private sector. This includes the capability to identify and share wallet data prior to losses occurring, including with blockchain analytics companies to facilitate the blocking of cryptocurrency wallets.

However, in the ACCC's experience, these organisations are generally unwilling to block or freeze wallets until law enforcement open an investigation, or an extensive assessment has been completed. The current capabilities and resourcing of law enforcement is such that the lead time for investigations is not relative to the speed of the crime, meaning money has often left Australia's jurisdiction before law enforcement have had the opportunity to obtain court orders requiring wallets to be blocked or frozen.

The ACCC recommends the introduction of innovative automatic risk-based processes for tracing and freezing cryptocurrency assets to increase the capability of law enforcement agencies to investigate and prosecute cybercrime. For example, initiatives in Singapore discussed below.

[2] Scamwatch report data 1 January to 26 November 2023.

Recommendation 2: Expansion of coordinated and timely intelligence sharing to combat cybercrime.

The ACCC recognises the importance of a coordinated effort to respond to the conduct of cybercrime and risks of cybercrime. The National Anti-Scam Centre was established by government to deliver a coordinated approach across government, industry, and law enforcement to combat scams. In the short term the National Anti-Scam Centre is enhancing information exchange through collaboration. In the medium term these efforts will be supplemented by the technology-based solution mentioned above.

To this end, the National Anti-Scam Centre has an Advisory Board comprising peak industry bodies, consumer organisations, victim support services, and law enforcement. It also has established a fusion cell and three working groups with membership drawn from law enforcement, government, private sector, and community organisations. Fusion cells are short term taskforces initiated to take timely action on specific, urgent problems relating to scams and financial crime. The coordination and intelligence sharing between sectors facilitated by the National Anti-Scam Centre has led to successful outcomes such as:

- using call diversion technology to break scammer-to-victim contact, reducing harm and the risk of further victimisation,
- collating best practice industry guidance on the use of intelligence to uplift and scale up investment scam disruption,
- identifying and taking down investment scam advertisements and websites, preventing further criminal activity,
- expanding best practice industry initiatives to block impersonation scams. This has been achieved by impersonated institutions sharing data with the National Anti-Scam Centre, which in turn passes confirmed investment-related cybercrime phone numbers to telecommunications providers to block, and
- sharing both trends and specific intelligence with law enforcement to support investigation and the prosecution of perpetrators of scams.

The National Anti-Scam Centre has seconded an intelligence analyst to the Joint Policing Cyber Crime Centre (JPC3) to enhance cooperation and intelligence information sharing between the National Anti-Scam Centre, Australian Federal Police (AFP), and other law enforcement organisations.

Coordinated and timely intelligence sharing is critical to combatting cybercrime and scams. The National Anti-Scam Centre has access to ReportCyber reports but is currently limited in how it can use the information. The National Anti-Scam Centre is developing an application programming interface (API) which will allow information reported to Scamwatch to be shared with ReportCyber, enabling victims to have their issues investigated without them having to report separately to both organisations.

Looking globally, the experience of Singapore's Anti-Scam Command during an operation earlier this year demonstrates the significant benefits of deliberate and timely collaboration between law enforcement, government agencies, and the private sector. Between 15 August and 15 September 2023, the Singapore Police Force and 6 partner banks sent more than 5,000 SMS messages to over 4,000 scam victims who are customers of the banks. This resulted in the successful disruption of more than 800 ongoing scams and averted potential financial losses of more than S$17.1 million (AUD$19.4 million). Key to this operation was the use of Robotic Process Automation (RPA) technology to disseminate crucial intelligence between the operation's partners. This enabled police to contact the bank's customers while the scam was still in progress, advising them to cease further transfers, and facilitated the distribution of compromised identifiers to the banks for blocking.

This commitment to collaboration between law enforcement and industry has been recognised by the Singapore Police Force as key to their cybercrime fighting capabilities. Since July 2022, six banks have co-located staff within the police Anti-Scam Command premises, enhancing police investigations through real time tracing of fund flow and freezing accounts. Since the co-location, proactive fund flow tracing into more than 40 scam cases has led to the seizure of more than S$1.5 million (AUD$1.7 million) from compromised bank accounts and wallets. Police report a recovery rate of over 60% due to these initiatives.[3]

Recommendation 3: Commitment to a 'no-wrong-door' approach to scam and cybercrime reporting, allowing victims to report to any appropriate entity and achieve the same outcomes.

Victims of cybercrime incur significant financial and emotional harm. Scam victims have a range of needs and often require financial assistance, mental health support, and legal or administrative guidance to navigate complaint processes and to remediate identity credentials or device compromise.

Supporting victims as soon as possible after the crime is important to prevent revictimisation. Scammers and cybercriminals frequently share or sell compromised identity data leading to victims being approached by nefarious third parties claiming the ability to retrieve lost funds. Rapid and extensive sharing of cybercrime intelligence is therefore essential to prevent revictimisation.

While there is undoubtably a role for Australia's law enforcement agencies in directly supporting victims of cybercrime, these efforts should draw on existing services where appropriate. The National Anti-Scam Centre is working to build and coordinate victim support capabilities, recognising that this is one of its key roles in the scams ecosystem. This enables law enforcement agencies to focus their resources on the work of detection, investigation, and prosecution of cybercrime. The ACCC would welcome the opportunity for the National Anti-Scam Centre to collaborate with law enforcement in developing approaches to scam victim support that draw on a wide range of services in a more coordinated way.

The optimal future state is a 'no-wrong-door' approach, where victims can report in any appropriate manner, be it through an official reporting mechanism such as Scamwatch or ReportCyber, or through notifying a relevant business or government agency. All actionable intelligence (including phone numbers, bank account details, and wallet addresses) is then shared with relevant private sector entities for disruption, with law enforcement for further investigation and prosecution, and with victim support services to support recovery and prevent revictimisation. The ACCC considers that the National Anti-Scam Centre has a key role to play in this future state for cybercrime related scams, including the coordination and maintenance of a consistent scams taxonomy to be used across all sectors. This work has begun under the auspices of the National Anti-Scam Centre's Data Integration and Technology Working Group.

Recommendation 4: Development of universal and enforceable mandatory codes for digital platforms, telecommunications companies, banks, and other payment providers.

The establishment of mandatory and enforceable industry codes that encompass banks, telecommunications providers, digital platforms, and cryptocurrency exchanges is required to ensure there are no weak links across the scams ecosystem.

Identity fraud is a complementary or enabling crime-type for scams and other cybercrime. Stolen identities are a key ingredient for scammers and other cybercriminals in sourcing a constant supply of new accounts for their illegal activities, and entities with the weakest

[3] https://www.police.gov.sg/Media-Room/News/20220906_opening_of_anti-scam_command_office Accessed 3 December 2023.

controls, such as certain online-only banks, online remitters, and digital currency exchanges are favoured. These are disproportionately represented in reports to Scamwatch as the recipients of stolen funds.

Under the existing frameworks, entities receiving stolen funds are not sufficiently incentivised to mitigate the risk of exploitation by scammers and other cybercriminals because they do not encounter significant financial liability or reputational risk for receiving stolen customer funds. Effective standards relating to know your customer obligations will be key in combatting scams and other cybercrimes.

More generally, it is the ACCC's view that effective standards must include three core characteristics:

- broad coverage,
- enforceability, and
- consistent and meaningful uplift to current scam mitigation practices.

It is the ACCC's experience that these characteristics are best achieved through mandatory codes. Such codes would be universal, enforceable, and apply clear minimum standards on digital platforms, telecommunications companies, banks, and other payment providers to:

- implement robust processes to protect customers from scams and identity misuse and prevent scammers using their services, including through effective utilisation of information in member banks' possession,
- clearly define the circumstance in which customers would be reimbursed or entitled to remedies for stolen scam funds, in circumstances where customers continue to bear losses that they have limited ability to prevent, and
- create transparent reporting on compliance with the framework, and independent enforcement and penalties for non-compliance.

The ACCC welcomes Treasury's current consultation process regarding mandatory industry codes concerning scams. The ACCC looks forward to the implementation of a robust joined-up approach that eliminates weak links in the scams ecosystem.

Recommendation 5: Law enforcement agencies leverage the National Anti-Scam Centre to deliver education and outreach activities in order to focus their own resources on investigation and prosecution of cybercrime.

One of the key capabilities of the National Anti-Scam Centre includes coordinating scam awareness activities by drawing on expertise across government, industry, and consumer organisations. The ACCC is conscious that more needs to be done to uplift scam education and awareness to better protect vulnerable communities and support victims. Current approaches are fragmented, and stakeholders have repeatedly called for national, well-coordinated campaigns that have broad reach, for example through television. Through the National Anti-Scam Centre, the ACCC is seeking to build consumer awareness of current and emerging scams and to ensure consumers know how to protect themselves.

The National Anti-Scam Centre responds to regular requests for printed copies of the publication, *The Little Black Book of Scams*, for distribution through various police stations and operational posts and will be producing more resources to support education and outreach activities to target diverse audiences.

The ACCC welcomes the Australian Federal Police's (AFP) presence on several key National Anti-Scam Centre forums covering communication and awareness raising regarding cybercrime generally and scams in particular. The ACCC also notes the AFP has Community Liaison teams in Melbourne, Sydney, Brisbane, Adelaide, and Perth that actively engage with diverse communities and vulnerable groups. The AFP is also very active on social media, recognising

that messages for scam and cybercrime awareness must be promoted on the various channels with which different segments of the community engage.

In addition to general awareness raising, targeted warnings regarding emerging scams is important. Both general and targeted messaging must be evidence based and informed by data.

Case study:

For example, in the first nine months of this year there were over 1,244 reports of, and $8.7 million in losses to a scam involving criminals posing as Chinese police. These scammers targeted, intimidated, and stole from Mandarin speaking young people studying in Australia. In August, the number of these reports doubled compared with previous months. The National Anti-Scam Centre escalated the issue to law enforcement and published a media release that reached approximately 10 million people. It was run by national and regional television broadcasters, radio stations and newspaper mastheads, and television interviews were conducted in English and Mandarin. The National Anti-Scam Centre shared the release with universities that have large international student communities. Furthermore, when intelligence analysis identified this scam was evolving to target Vietnamese speakers, the National Anti-Scam Centre engaged with a range of Vietnamese cultural and student groups and the Vietnamese Embassy, to circulate information to the community, including scams awareness information in Vietnamese on the Scamwatch website.

Similar intelligence-led awareness strategies have been developed in recent months in response to emerging scams targeting job seekers, and people purchasing new and used vehicles.

The National Anti-Scam Centre has been tasked by the Government to coordinate consistent messaging across the scams ecosystem to help consumers identify and avoid scams. The Scamwatch brand provides a well-recognised and strong platform to engage with consumers on education and awareness activities.

Through the National Anti-Scam Centre, the ACCC is increasing collaboration with community outreach conducted by Crimestoppers, often in conjunction with state and territory law enforcement agencies, as an opportunity to engage directly with the community.

The ACCC also encourages law enforcement to leverage the National Anti-Scam Centre to deliver education and outreach activities to focus more of its resources on investigation and prosecution of cybercrime.

Until recently, direct engagement between the National Anti-Scam Centre and state law enforcement has been ad hoc, though we are actively taking steps to ensure a more coordinated approach. The Northern Territory Police Force, New South Wales Police, Queensland Police Service, and Victoria Police are represented on the National Anti-Scam Centre's Scams Awareness Network. The latter three agencies plus South Australia Police and the AFP have recently accepted invitations to join the National Anti-Scam Centre's Emerging Trends and Responses Working Group. The objectives of this group include developing responses to new, emerging, and trending scams by:

- Prioritising education and awareness activities based on the best available data, information, and intelligence.
- Identifying the organisations and entities best placed to provide further intelligence to shape responses.
- Proactively seeking opportunities to provide timely awareness and education advice to the public.
- Developing and enhancing the National Anti-Scam Centre's and members' abilities to implement quick and coordinated responses to emerging scams.

As the working group's internal intelligence sharing processes become fully functional, law enforcement agencies' prevention and awareness efforts will benefit from up-to-date data and intelligence from the group's diverse membership. The ACCC believes this will create

opportunities to leverage the outreach and education actions of Australia's law enforcement agencies to further drive consistent scams awareness messaging to the community.

The ACCC welcomes the interest of other law enforcement agencies in participation in the National Anti-Scam Centre's Emerging Trends and Responses Working Group, as well as in the information sharing that membership enables.

Conclusion

The ACCC is committed to supporting Australia's law enforcement agencies in their vital work of detecting and investigating scams and other cybercrime and prosecuting those responsible. The ACCC believes the most effective way for it to support law enforcement to respond to scams and other cybercrime is through the National Anti-Scam Centre's data-sharing work and coordination of scam prevention activities and victim support. The ACCC welcomes further discussions on this topic and will provide any further assistance to the inquiry that may be required.

Should you wish to discuss any part of this submission, please contact , Executive General Manager of the National Anti-Scam Centre on .

Yours sincerely

Deputy Chair