Parliamentary Joint Committee on Law Enforcement

ANSWERS TO QUESTIONS ON NOTICE

Inquiry into the capability of law enforcement to respond to cybercrime October 2024

Agency:	Australian Competition and Consumer Commission
Question No:	
Topic:	**Education and awareness strategy**
Reference:	Written (14 November 2024)
Senator:	Helen Polley

Question:

6. The ACCC mentioned some of its education and awareness work at the public hearing on 22 October 2024. Is there an underlying strategy for this work at the ACCC, or any broader strategy to ensure the ACCC's work is coordinated with other agencies?

Answer:

- The National Anti-Scam Centre's strategy with respect to education and awareness focusses on six (6) priority cohorts:
  - First Nations Australians
  - Culturally and Linguistically Diverse
  - Older Australians
  - Youth
  - People living with Disability
  - Small Businesses
- The National Anti-Scam Centre's coordinates and collaborates closely with government and police on education and awareness for scams. A primary channel is Communications and Awareness Working Group (CAWG) which the National Anti-Scam Centre chairs.
- The CAWG is a working group and network consisting of 37 government, industry and consumer organisations who meet bi-monthly to discuss upcoming campaigns and aligned messaging. The aim of the group is to provide strategic input to effective communication, education, and outreach strategies to reduce the number of Australians caught by scams and reduce the losses to scams.
- CAWG outputs include coordinated and simplified protective messaging and the annual **Scams Awareness Week**.
- Scams Awareness Week is a consumer awareness campaign that reaches millions of Australians to educate them about scams. This year's campaign ran from 26 to 30 August with the theme 'Share a story, stop a scam'. Australians were encouraged to speak up, share and report scams to help protect others and reduce the stigma of being scammed.
- The National Anti-Scam Centre provides a wide range of campaign materials to support private and public organisations' participation in Scams Awareness Week. These materials, hosted on the Scamwatch website (www.scamwatch.gov.au), include social media assets, case studies, email banners, Microsoft Teams background, posters, videos of people who were real victims of scams telling their scam stories, and a series of videos featuring Monash Researcher and Neuropsychologist Dr Kate Gould.
- The National Anti-Scam Centre also conducts ongoing public awareness with regular media engagement. The National Anti-Scam Centre spokesperson ACCC Deputy Chair Catriona Lowe has appeared on ABC National, ABC Radio, 2GB, SBS, Sky News, 7

News, 9 News, 10 News, The Project, The Age, News.com.au, The Courier Mail and News Corps national in the period 1 June to 30 September 2024 (this is a non-exhaustive list).

- In addition, the Australian Government has funded the ACCC to develop an advertising campaign to drive community awareness of scams and communicate protective behaviours to guard against scammers. The campaign is being developed in accordance with the mandatory process for Australian Government campaign advertising. The campaign budget is expected to run the first half of the 2025 and stakeholder kits will be shared with government and private stakeholders to amplify the reach of the campaign.
- The Little Book of Scams is a key resource for our private, government and police partners use in a range of outreach contexts, such as at retirement villages or community seminars by crime prevention offices. Over 150,000 copies of the Little Book of Scams have been shared with government, police, private organisations and individuals between 01 January and 11 November 2024.
- The Little Book of Scams and scams awareness videos are also now available in 17 languages other than English. These languages are Arabic, Cantonese, Croatian, Dari, English, Farsi, German, Greek, Hindi, Indonesian, Italian, Korean, Macedonian, Mandarin, Spanish, Tagalog, Turkish, and Vietnamese.
- The National Anti-Scam Centre ran several stakeholder engagement workshops in late November 2024. The purpose of the workshops was to consult with state and federal government agencies, and relevant non-government agencies, regarding their existing outreach activities and explore the possibility of working with them to deliver key scams awareness information to at-risk audiences. This reflects that the National Anti-Scam Centre cannot reach our priority cohorts on its own and that such an approach would result in duplicative effort or the establishment of unnecessary channels for outreach.
- The National Anti-Scam Centre is also a member of the National Cybercrime Prevention Network, chaired by the Australian Federal Police. The National Cybercrime Prevention Network has similar goals to CAWG but with a remit to collaborate on awareness and prevention strategies for cybercrime.

Parliamentary Joint Committee on Law Enforcement

ANSWERS TO QUESTIONS ON NOTICE

Inquiry into the capability of law enforcement to respond to cybercrime October 2024

Agency: Australian Competition and Consumer Commission
Question No:
Topic: **ACCC fusion cells**
Reference: Written (14 November 2024)
Senator: Helen Polley

Question:

5. The ACCC mentioned fusion cells at the public hearing on 22 October 2024 (*Proof Committee Hansard*, p. 15). Could you please provide some more information about these fusion cells and what the ACCC has learned from them?

Answer:

- The National Anti-Scam Centre (NASC) leads time-limited public-private taskforces to counter specific scam problems. These taskforces are known as "fusion cells."
- By bringing together government, law enforcement, and representatives from the platforms and services exploited by criminals, fusion cells eliminate data silos and can disrupt the scam at all stages.
- A key aspect of the fusion cell model is the development of proof-of-concept disruption processes that extend beyond the life of the fusion cell.
- The first fusion cell targeted investment scams and was jointly led by the NASC and the Australian Securities and Investments Commission. The May 2024 final report on the fusion cell's achievements highlighted:
  - Collaboration with industry to develop referral processes for takedowns of scam advertisements and videos resulting in more than 1,000 scam advertisements and other inducements being removed by digital platforms.
  - Takedown of over 220 investment scam websites using the ASIC investment scam website takedown service.
  - Diversion to a recorded warning of 113 attempted calls by potential victims to confirmed imposter bond/term deposit scam phone numbers, and a further 548 following the fusion cell. Victims of this scam type lose an average of $265,000 and prevented losses are likely to be in the millions of dollars.
- Fusion cells are intended to have ongoing benefits and the Investment Scam Fusion Cell directly led to the following benefits:
  - The development of a new reporting form for reporting the scam advertisements which are the origin of many investment scams.
  - The development of machine learning techniques to proactively identify scam advertisements.
  - Development of automated referral process for investment scam websites to ASIC for takedown assessment.
  - The creation of a disruption handbook for AI trading platforms to create consistency in how organisations respond to AI trading platform scams.

  - Ongoing collaborations with Optus and Telstra to continue and expand recorded warnings to potential victims of high-loss imposter bond and term deposit scams.

- The public report on the outcomes of the Investment Scam Fusion Cell included a qualitative evaluation of the fusion cell, especially with respect to effective collaboration to produce tangible outcomes. This evaluation concluded that future fusion cells should emphasise the following features:
  - Greater time in establishing scope prior to the fusion cell initiation, with consideration to what is achievable in fusion cell timeframes.
  - Reliance on small working groups and emphasis on proof-of-concept exercises.
  - Terms of reference which require participants to report on the additionality of the fusion cell activities to establish a counterfactual scenario.
  - Greater emphasis on benchmarks for success in the initial weeks of the fusion cell.

- In terms of barriers to disruption, the most significant noted by participants was the need for widely adopted data-sharing infrastructure and clarity around legal uncertainties with respect to privacy and data-sharing. The NASC's funded program of work is delivering data sharing infrastructure. The second fusion cell has applied the lessons learned from the first in the development of the data sharing agreement it uses, to give participants confidence and clarity to proceed.

- The NASC's second fusion cell, focussed on job scams, will run for six months to March 2025. The objectives of the job scam fusion cell (which reflect the three pillars of the government's anti-scam strategy, prevention and disruption, consumer awareness, and victim support) are:
  - To disrupt job scams via:
    - Early identification of job scam campaigns and their enabling factors (digital platforms, fake websites, messaging apps, etc.),
    - Blocking or limiting scammers' ability to use enabling technology, products, and services,
    - Developing strategies to stop consumers sending funds, and
    - 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.

- Lessons learned from the first fusion cell, specifically those noted in the evaluation process above, have been implemented in the second fusion cell, in a range of ways, including:
  - Establishing multiple working groups as the "engine" of the fusion cell, to achieve the key pieces of work required. These small groups are more agile and effective in acting on data and trends than larger meetings of the whole fusion cell.
  - Early work on co-designing the scope and priorities of the fusion cell. Drawing on lessons learned, an in-person workshop was held to align priorities, measures of success, and objectives for the fusion cell and each working group.
  - Regular progress updates between fusion cell working groups, and to key stakeholders to guard against "siloing" of knowledge and intelligence.
  - Sharing data using the National Anti-Scam Centre Partner Portal. Sharing by other means such as email was identified as unsatisfactory by participants in the first fusion cell. This new process will enable the submission of scam identifiers (email addresses,

bank account details, etc) to the National Anti-Scam Centre for analysis and disruption.

Parliamentary Joint Committee on Law Enforcement

ANSWERS TO QUESTIONS ON NOTICE

Inquiry into the capability of law enforcement to respond to cybercrime October 2024

Agency: Australian Competition and Consumer Commission
Question No:
Topic: **Assistance for scam victims**
Reference: Written (14 November 2024)
Senator: Helen Polley

Question:

4. At the public hearing on 22 October 2024 (*Proof Committee Hansard*, p. 17), the ACCC said one of the primary functions of Scamwatch reports is intelligence-based. Does the National Anti-Scam Centre connect scam victims with law enforcement or IDCARE, or provide any other assistance?

Answer:

The National Anti-Scam Centre receives reports from victims through its Scamwatch online reporting service. About 8.1% of people who report to the service advise that they have incurred a financial loss to a scam.

The National Anti-Scam Centre (NASC) receives information from law enforcement in Australia and overseas about Australian victims identified in investigations of scams. We have processes in place with key stakeholders (including law enforcement) to notify victims and provide advice and referrals to support services.

Connection with law enforcement

The NASC is working with representatives from law enforcement including through the Joint Policing Cybercrime Coordination Centre (JPC3) and with the Australian Signals Directorate (ASD) to facilitate the direct referral of victim reports that are made to Scamwatch where it appears to be a crime.

The NASC has an employee seconded to the JPC3 and regularly shares information and intelligence to support law enforcement. The NASC facilitates welfare checks in a small number of cases through law enforcement via Local Area Commands.

The NASC has worked with the Australian Federal Police (AFP); the JPC3 and regulators such as the Australian Securities and Investments Commission to set up victim notification processes. This process aims to provide awareness and support to victims that are identified as a result of law enforcement investigations here and overseas. Over 20,000 victims have been contacted as part of these processes since 1 July 2024.

Support for victims and referral to services

Depending on the scam reported, victims receive automated tailored advice which will refer them to the relevant services for the scam type. In a small number of cases, NASC staff contact individuals directly (by email or phone) where they may be needing urgent assistance or experiencing a mental health crisis. The aim of the contact is to assist them to get to the services that can assist them, for example a local financial counsellor, LifeLine or other mental health services or Services Australia (in the event of MyGov account compromise).

From 1 July 2024 to 28 November 2024, the NASC has sent 940 emails to victims and contacted over 60 by phone.

When reporting to Scamwatch, victims who report financial loss over $5000 or identity theft are offered direct referral and contact by IDCARE. Where they consent, the NASC shares information with IDCARE so that it can provide follow up contact where IDCARE considers it is necessary. From 1 July 2024 more than 3,300 people have been referred to IDCARE from Scamwatch.

Parliamentary Joint Committee on Law Enforcement

ANSWERS TO QUESTIONS ON NOTICE

Inquiry into the capability of law enforcement to respond to cybercrime October 2024

Agency:	Australian Competition and Consumer Commission
Question No:	
Topic:	**Review of Scamwatch reports**
Reference:	Written (14 November 2024)
Senator:	Helen Polley

Question:

3. The ACCC advised that there is a manual review of five to ten per cent of Scamwatch reports (answers to questions on notice, 4 June 2024, received 26 June 2024). Could you please clarify what level of review is conducted of other reports?

Answer:

Reports that are not subject to an immediate manual review are recorded for statistical analysis and are used for intelligence purposes. These may be subject to review at a later time as required in relation to targeted specific programs of work or areas of focus.

Scamwatch receives hundreds of reports per day from members of the public. We are unable to review all reports received, so prioritise those we do based on factors such as harm caused by the scam (both financially and in terms of loss of personal information), vulnerability of groups impacted by the scam, and novelty/increasing trends observed in the scam methodology or impersonation target. We use a range of methodologies to identify trends, including identifying clusters of the same impersonation target, scam type, contact method or payment method above a baseline level.

Report reviews allow us to develop a more complete intelligence picture and produce better insights for various National Anti-Scam Centre outputs. These outputs include media releases (see: https://www.nasc.gov.au/news), contributions to routine reporting such as the Targeting Scams Report and Quarterly Updates of the National Anti-Scam Centre, and intelligence briefs for Government and Industry partners. We work to develop intelligence that is of benefit to the operations of our partners and can support protections for the consumers they serve.

Parliamentary Joint Committee on Law Enforcement

ANSWERS TO QUESTIONS ON NOTICE

Inquiry into the capability of law enforcement to respond to cybercrime October 2024

Agency:	Australian Competition and Consumer Commission
Question No:	
Topic:	**Scamwatch reports**
Reference:	Written (14 November 2024)
Senator:	Helen Polley

Question:

1. At the public hearing on 22 October 2024 (Proof Committee Hansard, p. 17), the ACCC said most people who report to Scamwatch are altruistic reporters. What proportion of Scamwatch reports are from victims affected by a scam compared with those who saw the scam but were not affected by it? Is there any other related data you can provide?

Answer:

Scamwatch records whether reporters have suffered a financial loss, lost personal information to a scammer or lost both.

From 1 January to 30 September 2024, Scamwatch received **198,126 reports**. Of these **166,633 (84.1%) were from altruistic reporters** in the sense that the reporters did not record that they had lost any personal information or money to the scam. In some instances, the reporters are not sure if it is a scam. The remainder, 31,493 (15.9%) reported either financial or personal information (or both) being stolen by the scammer.

The National Anti-Scam Centre also provides a service where the public can report scam websites or advertisements they see. These are all altruistic reports. Since the service commenced in July and August there have been 1,611 reports about ads or websites made through this service.

Parliamentary Joint Committee on Law Enforcement

ANSWERS TO QUESTIONS ON NOTICE

Inquiry into the capability of law enforcement to respond to cybercrime October 2024

Agency:	Australian Competition and Consumer Commission
Question No:	
Topic:	**NASC Information sharing**
Reference:	Written (14 November 2024)
Senator:	Helen Polley

Question:

2. The ACCC has given evidence about information sharing between the National Anti-Scam Centre (NASC), law enforcement, government, and the private sector (answers to questions on notice, 4 June 2024, received 26 June 2024; and *Proof Committee Hansard,* 22 October 2024, p. 17).

(a) Could you provide more detail about the NASC's current information sharing arrangements and any timelines for further improvements?

(b) Since the ACCC's 26 June 2024 answers to questions on notice, could you provide an update on work to share Scamwatch reports with ReportCyber in near real time, and for ReportCyber reports to be integrated into the NASC's 'dataverse'? Has this been implemented and is it effective?

(c) The ACCC recommended a 'no wrong door' approach (*Submission 17,* p. 4). How would this be implemented with existing reporting options? Is work underway to do so and when is this expected to occur?

Answer:

(a) The National Anti-Scam Centre (NASC) was established on 1 July 2023 by the Australian Government to make Australia a harder target for scammers. The NASC's data and information sharing capability supports disruption, prevention and awareness raising activities.

Currently, the NASC employs a range of tools to ensure scam reports and intelligence are provided to – and obtained from - relevant private and public sector organisations. These include:

- Providing scam information and suspect BSB and account numbers from Scamwatch reports to the financial sector via the Australian Financial Crimes Exchange (AFCX) at regular intervals each day (where the reporter has consented for that information to be provided to financial services organisations).
- Receiving scam information about suspect websites from participating members of the AFCX intelligence loop.
- Providing information from Scamwatch reports through an automated process to MoneyGram and Western Union on a weekly basis about scams, citing these as the payment method (where the reporter has consented for that sharing).
- Providing all alleged suspect phone numbers and sender IDs reported two or more times to Scamwatch each week (text or phone call scams) with 11 telecommunication services providers and the Australian Communications and Media Authority.
- Receiving information from some of the telecommunications service providers about actions taken.

- Automated daily sharing of suspect Facebook scam URLs reported to Scamwatch about scams on the Meta platform with Meta (where the reporter has consented, the reporter nominated Facebook as the contact method for the scam and the reporter supplies their Facebook profile address).
- Automated weekly sharing of Scamwatch reports occurring on the Gumtree platform with Gumtree (where consent provided).
- Receiving weekly or fortnightly (varies) updates from Gumtree on actions taken and on scam activity on the platform.
- Automated daily sharing of Scamwatch reports about investment scams with ASIC (via API); this includes investment scam website URLS to enable ASIC to assess for takedown, and consider issuing warnings about.
- Receiving information from ReportCyber (covered further in (b) below).
- Providing scam information to IDCARE where scam victims who report to Scamwatch are seeking support (and consent to their information being shared) daily through an automated process.

The NASC also shares scams information monthly with the ACMA, the US Federal Trade Commission's Sentinel Network and NBN Co, including a cryptocurrency focussed monthly report shared with ASIC. Further, tailored intelligence products are developed and shared with relevant industry associations in relation to specific and trending scams (e.g. sending details of cryptocurrency wallets that may be being used in scams to Australian cryptocurrency exchanges) and with law enforcement.

The development of the Government's Scams Prevention Framework, which is currently being considered by Parliament, will impose obligations on entities in designated sectors to share actionable scam intelligence with the ACCC (as Framework regulator). The NASC is focussing on banking, digital platforms, and telecommunications service providers as the data stakeholders likely to be the first regulated entities under the Framework. The NASC will host information sharing workshops with these first entities in December 2024 and early 2025. While the commencement date, reporting requirements and timing under the Framework are not yet finalised, the NASC is working to be ready for implementation in 2025.

(b) The NASC (ACCC) has been receiving data from ReportCyber for many years, under a memorandum of understanding. The NASC intelligence team is working with technology specialists to upgrade capability to fully integrate the ReportCyber data into the NASC dataverse.

The NASC has built an Application Programming Interface (API) to enable Scamwatch reports to be accessed by law enforcement through the Australian Signals Directorate's (ASD's) ReportCyber platform. The Scamwatch information will be available to law enforcement officers on-demand, that is, when they select to see the data from ReportCyber's interface. The source data is refreshed daily. Sharing NASC data with ReportCyber will mean police jurisdictions can query the NASC database for scammer identifiers relevant to their investigations into scam criminal activity. Work is continuing to test and refine the API, and information sharing will be covered by a data sharing agreement between ASD and the ACCC. Once the legal requirements are complete, the updated ReportCyber platform with integrated NASC data will be enabled.

Current sharing (from ReportCyber to the NASC) has been effective to better understand scams and informs public communication on scams such as the annual Targeting Scams report. The NASC is in discussions with the Australian Federal Police about information sharing more broadly, as well as with some State police agencies who are interested in integrating intelligence into the NASC website takedown service.

(c) The NASC's approach to 'no-wrong-door' focuses on ensuring that no matter where a consumer reports a scam the actionable intelligence reported can be shared and actioned. This includes reporting through Scamwatch or ReportCyber, or through a relevant business or government agency. Actionable scam 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.

In circumstances where consent is provided the NASC may also share victim/reporter information with private or public organisations (for example so they can access support services). However, currently most organisations do not have these consent arrangements in place to share victim or reporter level information with the NASC. Given the careful balancing required to limit the necessary sharing of personal information across the ecosystem and sharing enough information to stop scams, the NASC has focused its 'no wrong door' approach on actionable intelligence rather than victim reporting.

The data partnering and technology work to support the 'no wrong door' approach is well underway and will bring more government and private sector partners on board to provide and receive scam data and intelligence. The development of the Scams Prevention Framework will see banks, telecommunications providers and digital platforms as a key focus in the short term.