

Parliamentary Joint Committee on Law Enforcement

ANSWERS TO QUESTIONS ON NOTICE

Treasury Portfolio

Inquiry into the capability of law enforcement to respond to cybercrime

Agency: Australian Competition and Consumer Commission
Question No: 1 - 3
Topic: Scam reporting and analysis
Reference: Written, (4 June 2024)
Senator: Senator Polley, Chair

Questions:

Questions from Senator Polley, Chair:

It was suggested to the committee that there is a need to analyse ReportCyber reports to find shared characteristics and identify reports that may relate to the same criminal group or scam (Committee Hansard [Proof], 23 May 2024, p. 23).

1. Regarding ScamWatch reports to the National Anti-Scam Centre, can you please advise what level of analysis is done on reports to detect patterns?
2. Does the analysis also consider reports made to ReportCyber?
3. How is this analysis shared to inform law enforcement's response to the reports.

Answers:

Q1. Regarding ScamWatch reports to the National Anti-Scam Centre, can you please advise what level of analysis is done on reports to detect patterns?

- The National Anti-Scam Centre's Scamwatch receives approximately 800 reports from the Australian public per day. Most reports to Scamwatch have no or low loss amounts (under \$1000).
- Currently the National Anti-Scam Centre manually reviews Scamwatch reports to:
 - verify high loss amounts or connection to Australia (for example overseas reporters); and
 - for duplicates
- This manual review amounts to 5-10% of reports. This review also may also identify increases in scam types with high losses such as foreign authority threats scams or frequently appearing scammer names/aliases, emails, websites, and phone numbers related to high loss investment scams. Where possible this information is referred to industry or law enforcement for disruption and investigation.
- In addition, the National Anti-Scam Centre analysis Scamwatch reports for trends and patterns in:
 - report numbers and losses against scam type, scammer contact method, scam payment method and reporter demographics
 - common enablers, such as particular banks, digital platforms, telecommunications providers and software providers scammers might be using.

- The National Anti-Scam Centre also receives intelligence from government and industry partners of trends they are observing, which may prompt further analysis of Scamwatch data.
- Data analysis underpins all of the work of the National Anti-Scam Centre. It uses its analysis to inform public awareness campaigns and to engage with industry and law enforcement on specific disruption or protections measures that might be adopted.
- The National Anti-Scam Centre's public reports (Targeting Scams Report¹, Fusion Cell Report², and Quarterly Reports³) provide more detail of this analysis and actions taken.
- The National Anti-Scam Centre also uses its analysis to prepare intelligence briefs for committees, advisory boards and law enforcement.

Q2. Does the analysis also consider reports made to ReportCyber?

- Since December 2023, the National Anti-Scam Centre has been receiving ReportCyber reports automatically daily. Work is continuing to integrate these reports into the National Anti-Scam Centre's dataverse to enable more comprehensive analysis. This is planned for completion within Quarter 1 of 2024/2025.
- The National Anti-Scam Centre also has access to the Australian Signal Directorate's ReportCyber Application Platform (RCAP) which provides graphs and charts of scam losses and categorical breakdowns.

Q3. How is this analysis shared to inform law enforcement's response to the reports.

- The National Anti-Scam Centre is progressing automated sharing of Scamwatch reports in near real-time to ReportCyber to enable police to conduct enquiries across the Scamwatch reports to inform and be used in investigations. This is also scheduled for completion by Quarter 1 of 2024/2025.
- The National Anti-Scam Centre has a secondee who works 2 days per week in the Joint Policing Cybercrime Coordination Centre (JPC3) which enables the sharing of information to inform law enforcement prioritises. A member of the AFP is also on the National Anti-Scam Centre's Advisory Board.
- The National Anti-Scam Centre also receives requests from law enforcement periodically for Scamwatch report data and provides this.
- At present, the National Anti-Scam Centre periodically share intelligence with law enforcement when emerging threats are identified in Scamwatch data.
- In addition to direct feeds of all Scamwatch data to ReportCyber, the National Anti-Scam Centre is exploring options for uploading scam threat vectors to the ASD's Cyber Threat Intelligence Sharing (CTIS) to support Policing agencies with near real-time feeds of scammer details.

¹ See the series here: <https://www.accc.gov.au/about-us/publications/serial-publications/targeting-scams-reports-on-scams-activity>

² The first Fusion Cell Report can be found here: <https://www.accc.gov.au/about-us/publications/serial-publications/national-anti-scam-centre-fusion-cell-report>

³ See the series here: <https://www.accc.gov.au/about-us/publications/serial-publications/national-anti-scam-centre-quarterly-update>