Tasmania Police

TASMANIA POLICE SUBMISSION – INQUIRY INTO COMBATTING CRIME AS A SERVICE

Tasmania Police has a Cybercrime Unit (CCU) of one Detective Sergeant and two Detective Constables responsible for both cyber-dependent and cyber-enabled crimes. Tasmania relies on additional support provided by the Joint Policing Cybercrime Coordination Centre (JPC3) and interstate police where required.

Tasmania Police CCU manage all reports received via the national REPORTCYBER reporting platform (Australian Cyber Security Centre) and investigate on average 1600 reports a year.

ToR (a) The nature and impact of these and other technology-driven advancements on criminal methodologies and activities, including the use of cryptocurrencies.

ToR (b) The impact of these types of technology-driven crimes on Australians, including with regard to age, gender, socio-economic status and business type.

Tasmania Police has observed a small reduction in reported cybercrime via the REPORTCYBER platform (10% over previous 3 years), although significant losses are still being reported by victims. Romance scams, investment scams, business email compromises (BEC) and low-level marketplace scams are the biggest threat to the wider community and still prevalent. Many victims are suffering lifelong financial hardship as a result.

Tasmania Police has assessed that the increasing presence of cryptocurrency ATMs (CATMs) in Tasmania is further enabling overseas criminals to target Tasmanians involved in scams. Scammers are able to leverage CATMs to circumvent fraud restrictions placed on the users. Tasmania Police participated in a national operation to combat the use of CATMs by scam victims. No legitimate CATM activity was identified, and all users were found to be involved in scams with moderate to severe financial impacts.

Denial of service attacks, data theft and ransomware attacks have significant impact on business, government and critical infrastructure. Statistics indicate these crime types are under reported by victims, likely to protect reputational harm.

The emerging threat is consistent and ever changing. New threats are increasing at an alarming rate as the result of new technological advancements.

The evolution of deepfake technology, powered by advancements in generative Artificial Intelligence (AI) will transform the digital landscape and create significant challenges for law enforcement.

The rapidly rising threat of AI is of significant concern not only to chief information security officers (CISOs) but the threat to the public is increased. Malicious actors will utilise AI power to socially engineering and contact scam victims. This will enable scammers to significantly increase volume by reducing the need for human staffed 'boiler-room style call-centres.' Personalised attacks on victims will be completed on a speed and scale never seen with use of AI to impersonate businesses, employees and other family members.

ToR (c) Challenges and opportunities for Australian law enforcement in combatting these and other evolving criminal methodologies.

Legislation has not kept pace with technological change. Restrictive search powers are currently under review. Tasmania Police are often reliant on the provisions of Commonwealth legislation and powers.

Tasmania Police has a cryptocurrency draft policy under review to enable the lawful seizure, storage and disposal of cryptocurrency. Legislative change is also being proposed to facilitate this policy.

An opportunity exists to enable review of legislation nationally and build an effective legal framework that empowers law enforcement and enables the prosecution and disruption of cybercrime.

Opportunities to combat these criminal methodologies also exist within community engagement. Tasmania Police works closely with the AFP led JPC3 Cyber Prevention team to ensure consistent and contemporary messaging is distributed to victims via the correct channels and stakeholders. Tasmania Police participate in all national campaigns and collaborate and engage closely with local media, community groups, schools and the wider public to provide education and prevention messaging to reduce the incidences of cybercrime in the community. The second National re_B00TCMP was hosted by Tasmania Police in 2025, with over 30 youth participants from around Tasmania.

ToR (d) Whether the existing legislative, regulatory, and policy frameworks to address these and other evolving criminal methodologies are fit for purpose.

Under current arrangements the Australia Federal Police coordinate major incident responses; IDCare and Scamwatch and REPORTCYBER contribute intelligence and victim support.

Currently the integration of Scamwatch data into REPORTCYBER is being explored as are further analytical tools to analyse data and reports to implement barriers and identify immediate cybercrime threats.

A single host '*National Portal'* to receive all reports of cybercrime would allow central point analysis, complaint referral and freezing of assets on receipt of a report. This would also ensure consistent victim care, public alerts, and allow remote access to intelligence for all law enforcement agencies enabling partnerships nationally to target the fight against cybercrime in a more cohesive manner. It is essential this be underpinned by an effective

legal framework that empowers law enforcement and enables the prosecution and disruption of cybercrime.

Relationships with the financial sector are improving with a strong collaboration with groups such as the Economic Crime Forum (ECF). The early identification and disruption of known money mule accounts is essential in the remediation of victim funds and prevention of lost funds offshore.

There is a need to further reduce barriers in the attainment of information from the financial sector to allow attribution to bank accounts. Amendments to strict privacy legislation and better sharing of AUSTRAC information (SMRS) would improve information sharing between law enforcement and financial institutions likely resulting better disruption and recovery of funds and identification of offenders.

Financial institutions differ in their interpretation of Australian Privacy Principle 6.2(e) of the *Privacy Act 1988* for the disclosure of personal information to law enforcement resulting in a further lengthy legal request