South Australia Police submission to
Australia's Parliamentary Joint Committee on Law Enforcement

INQUIRY INTO THE CHALLENGES AND OPPORTUNITIES FOR AUSTRALIAN LAW ENFORCEMENT IN COMBATTING CRIME AS A SERVICE.

On behalf of South Australia Police (SAPOL), I welcome the opportunity to provide a submission to the Committee. This submission outlines the importance of ongoing cooperation between law enforcement and both government and non-government partners in addressing Crime as a Service.

Nature and Impact of Technology-Driven Advancements including cryptocurrencies.

While the term "Crime as a Service" is often used to describe this evolving threat landscape, it is important to clarify crime itself is not a subscription-based model. Offenders are increasingly exploiting service-based technologies, such as cloud infrastructure, anonymising tools, and cryptocurrency platforms to outsource and automate elements of their operations. This shift enables even low-skilled actors to engage in sophisticated criminal activity, posing new challenges for law enforcement. This includes offerings such as ransomware as a service, phishing as a service, and access brokers who sell compromised entry points into networks. These services are increasingly "turnkey" meaning they are prepackaged, ready to deploy solutions requiring minimal technical skill from the end user. This lowers the barrier to entry for criminal actors and enables scalable, repeatable attacks.

Recent national operational disruptions including the dismantling of LockBit (ransomware) infrastructure and the takedown of LabHost (phishing) demonstrate the global reach and resilience of these criminal platforms. These cases reflect the emergence of a platform economy in organised cybercrime, where illicit services are modular, monetised, and supported by customer service models.

Artificial Intelligence is accelerating criminal tradecraft, enabling threat actors to rapidly generate phishing kits, fabricate personal identities, and produce Artificial Intelligence (AI) generated Child Sexual Abuse Material (CSAM). These capabilities are increasingly being integrated into Crime as a Service ecosystems, where tools and services are modular, scalable, and accessible to nontechnical users. The production and distribution of AI generated CSAM including deepfake imagery and synthetic media, presents significant challenges for law enforcement, particularly in detection, attribution, and evidentiary validation.

Unlike traditional forms of CSAM, AI generated content may not involve direct victimisation at the point of creation, complicating legal and investigative pathways. The blurred lines between real and AI generated CSAM, combined with the speed and anonymity of digital platforms, require new approaches to digital forensics, victim identification, and platform accountability.

Crime as a Service is no longer confined to cybercrime. Offenders now exploit service-based models to facilitate both online and offline harm. This includes emerging threats such as Sadistic Online Exploitation (SOE), where offenders share

coercion methods and content within closed networks and real-world violence for notoriety. These developments highlight the convergence of cybercrime, child exploitation, and violent extremism within a single service economy, demanding a coordinated national response.

Cryptocurrencies continue to serve as the primary payment method within Crime as a Service ecosystems, enabling fast, borderless transactions with obfuscation features such as mixers, privacy coins, and rapid exchange services. Unlike traditional banking systems which operate within regulated environments with standardised identity verification, transaction monitoring, and reporting obligations, the digital asset landscape presents distinct challenges for law enforcement.

The use of hot wallets (online and actively used for transactions) and cold wallets (offline and often hardware based for secure storage) complicates the identification, tracing, and seizure of illicit assets. Digital Currency Exchanges (DCEs) also vary widely in terms of jurisdiction, compliance maturity, and cooperation with law enforcement, which can affect the availability and reliability of transactional data.

These structural and operational differences require specialised investigational capabilities, including technical expertise, legal pathways, and cross sector cooperation to effectively respond to cryptocurrency enabled criminal activity.

Challenges and Opportunities for Australian Law Enforcement

SAPOL faces a growing challenge in keeping pace with the speed and sophistication of technology enabled crime. One of the most pressing issues is the mismatch between the speed at which offenders can move illicit funds and the time it takes investigators to access the necessary data to intervene. Criminals operating within digital ecosystems, particularly those using DCEs and instant exchangers can cash out within minutes, while law enforcement often faces delays in obtaining cross border data or responses from service providers. This gap undermines very short timeframes for freezing assets and recovering funds.

Despite improvements in protocols, asset freezing remains inconsistent across institutions. Banks and DCEs apply varied criteria, operate on different schedules, and offer uneven escalation pathways. While informal contact directories and working relationships exist between SAPOL and financial institutions, these are not standardised nationally nor universally adopted. Establishing formal, government backed agreements with clearly defined “always on” escalation channels would improve the speed and reliability of fund recovery efforts, particularly in high-risk or time sensitive scenarios.

SAPOL faces growing demand for blockchain forensic expertise to investigate cryptocurrency enabled crime. SAPOL is currently building expertise in this area using cryptocurrency analytics and open-source tracing. To strengthen our capability, SAPOL proposes an internal structured program to build local expertise, including regular controlled tracing exercises to test skills and ensure evidence meets court standards.

Recent national operations such as Cronos (LockBit), Cookie Monster (Genesis Market), and the LabHost takedown show that targeting the infrastructure behind

cybercrime delivers the greatest impact. These actions removed criminal services, froze illicit funds, and produced valuable intelligence for further investigations. SAPOL can play a stronger role in these national and international efforts by embedding disruption as a core part of our policing strategy.

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

The increasing prevalence of cybercrime facilitated through foreign-owned online platforms presents significant challenges for Australian law enforcement, particularly in accessing electronic evidence stored offshore. To address this, the Australian Government has implemented the International Production Orders (IPO) framework, enabling law enforcement agencies to directly request electronic data from communications service providers in countries with which Australia has a designated agreement. The agreement allows Australian agencies to issue IPOs directly to international providers, streamlining access to evidentiary data for investigations into serious crimes, including cybercrime.

While SAPOL is not yet a direct user of the IPO mechanism, its integration should be considered as part of SAPOL's future capability development. Aligning with these contemporary instruments would ensure timely, lawful, and effective access to cross border digital evidence. This would significantly increase jurisdictional coordination and investigative ability, particularly in cases involving transnational digital infrastructure and emerging threats.

Cybercrime investigations in South Australia are often limited by the ability to lawfully access cloud-based evidence. Where a Commonwealth offence is identified, SAPOL works with Commonwealth authorities to obtain relevant data. In cases where no Commonwealth offence applies, access is restricted to matters involving child exploitation. Outside of these circumstances, SAPOL can only access cloud-based data with the consent of the account holder or entity that controls the data.

This issue has been formally raised with the South Australian Attorney General's Department, and SAPOL awaits further guidance. To ensure law enforcement can respond effectively to evolving digital threats, legislative reform is needed to expand lawful access to cloud based evidence, clarify jurisdictional authority, and support the integration of national and international data sharing mechanisms.

[redacted]

Grant Stevens LEM APM
COMMISSIONER OF POLICE

9 October 2025