Parliamentary Joint Committee on Law Enforcement – Inquiry into Combatting Crime as a Service

Submission from the Queensland Police Service

Contents

1. INTRODUCTION

The Queensland Police Service's (QPS) written submission addresses the terms of reference for the Australian Parliament's Parliamentary Joint Committee on Law Enforcement's *Inquiry into Combatting Crime as a Service* (the Inquiry) to inform its deliberations and findings. The QPS welcomes the opportunity to contribute to the Inquiry.

This submission reflects factual information from the QPS and related services only and is not a whole-of-Government submission. This submission does not comment on the current legislation in Queensland which may be relevant to matters being explored by the Inquiry.

2. BACKGROUND: THE QUEENSLAND POLICE SERVICE

The QPS is the primary law enforcement and community safety agency for Queensland. It fulfils this role throughout the state, 24 hours a day, seven days a week, 365 days a year, upholding the law and assisting the community, particularly in times of emergency, disaster and crisis.

The QPS is responsible for the functions of policing and community safety, State Emergency Service and Marine Rescue Queensland.

The QPS is Queensland's primary law enforcement agency. Under the *Police Service Administration Act 1990*, the functions of the QPS are:

- preserving peace and good order in all areas of Queensland;
- protecting and supporting the Queensland community;
- preventing and detecting crime;
- upholding the law;
- administrating the law fairly and efficiently; and
- bringing offenders to justice.

The QPS continues to operate within a dynamic and uncertain environment as Queensland, like many jurisdictions globally, contends with post-pandemic socio-economic challenges exacerbated by our uniquely decentralised population. Spanning over 1.7 million square kilometres, the vast territory of Queensland requires adaptive strategies to ensure community safety across our state. As a result, the QPS is being challenged to meet the ever-evolving demands for our service. The QPS delivers its core responsibilities through our frontline policing services that are spread throughout Queensland and are managed as 15 distinct police districts.

Our frontline is supported by specialist detectives and officers in the Crime and Intelligence Command. The Crime and Intelligence Command delivers an enhanced intelligence and investigative for frontline policing through;

- Challenging the current operating environment through a collaborative lens
- Maintaining the specialities of crime and intelligence and continue to build regional capability
- Greater understanding of the influences impacting on the QPS environments
- Prioritising resources for greatest impact on crime and support to frontline
- Discovering opportunities to build on future capacity
- Enhancing the prevention and disruption strategies to reduce the impact of crime on the community, and
- Remaining the central point of contact for interstate, international, government and industry partners for matters pertaining to serious and organised crime.

For more information in relation to the functions and capabilities of the QPS, the committee may be interested in our QPS external website and our latest annual report that can be found here:

Queensland Police Service

Annual Report 2024-2025 | QPS

3. PURPOSE

This summary outlines key challenges for the QPS and its response to emerging crime methodologies, particularly the rise of Crime as a Service (CaaS).

Topics and sub-topics

1. **Money Laundering and Cryptocurrency**
   a. Cryptocurrency automatic teller machines
   b. Physical attacks targeting cryptocurrency users
2. **Physical world offending via CaaS – Serious Crime/Illicit Tobacco/Firearms**
   a. Illicit tobacco – use of encrypted devices
   b. Firearms – privately made firearms and 3D printing
3. **Scam/Phishing-as-a-Service**
   a. The role of Subscriber Identity Module (SIM) boxes in facilitating phishing scams
4. **Ransomware and Cyber Extortion**
   a. The role of ransomware and Cyber Extortion in facilitating crime
5. **Online Child Abuse**
   a. Pay-per-view child abuse content.
   b. Sadistic online exploitation.

4. MONEY LAUNDERING AND CRYPTOCURRENCY

4.1 Cryptocurrency automated teller machines (CATMs)

How it works

CATMs allow users to convert cash into digital currencies primarily Bitcoin, Tether and Ethereum. Australia has the highest number of CATMs in the Asia Pacific region, and is the third largest hub for CATMs globally, behind the United States and Canada. These machines are located in convenience stores, petrol stations, and shopping centres, enabling fast, pseudonymous transactions to digital wallets.

QPS challenges

- **Money laundering by organised crime groups (OCGs):** CATMs are being exploited by OCGs to launder illicit funds, bypassing traditional financial oversight.
- **Anonymity and speed:** Pseudonymous, irreversible transactions hinder tracing of illicit funds.
- **Regulatory gaps:** Some CATMs are linked to offshore exchanges, which poses law enforcement challenges.
- **Scam facilitation:** Victims of romance, investment, and ransomware scams are directed to deposit cash into CATMs, unknowingly aiding criminal operations.

- **Money mule exploitation:** Vulnerable individuals are being coerced into acting as money mules (e.g., individuals recruited or coerced to deposit drug-related cash into CATMs, distancing traffickers from direct involvement).

QPS actions

- Collaborate with Australian Transaction Reports and Analysis Centre (AUSTRAC) to identify high-risk CATM operators and users through transaction monitoring and intelligence sharing.
- Support enforcement actions against non-compliant CATM operators and suspected money mules.
- Deploy prevention messaging near CATMs, warning about scams and encouraging reporting.
- Target education campaigns at older demographics, who represent over 70% of CATM transaction value.

Queensland impacts

- Queensland has increasing exposure to crypto-related scams and laundering, with Australia being the fastest-growing market for CATMs. Australia is home to over 1,800 CATMs with more than 200 located in Queensland.
- QPS has participated in national operations, identifying both scam victims and suspected offenders.
- AUSTRAC and Australian Federal Police (AFP) identified over 90 high-risk CATM users in an Australia wide investigation including Queensland residents.
- AUSTRAC analysis confirmed 10% of CATM transactions may be linked to illicit activity (drug trafficking, scams, organised crime), with some activity coordinated by international networks, including state-backed actors targeting vulnerable people.

Examples

- **Queensland-led investigation:** The Queensland Joint Organised Crime Taskforce (QJOCT) uncovered a laundering scheme using a security company's armoured cash unit to convert ~$190 million into cryptocurrency via front businesses, blending legitimate and illicit funds.

4.2 Physical Attacks Targeting Cryptocurrency Users (Wrench Attacks)

How it works

A 'wrench attack' involves physically coercing a cryptocurrency holder, often through violence or intimidation to reveal wallet credentials or conduct live transactions. These attacks bypass digital security by exploiting human vulnerability, often targeting individuals identified via social media or public crypto affiliations.

QPS challenges

- **Rising threat in Queensland**: Wrench attacks are likely to increase locally, mirroring global trends driven by rising crypto valuations and poor personal security practices.
- **Limited online monitoring**: Criminals use social media and forums to profile targets, with minimal oversight or early detection capabilities.

- **Complex investigations**: These hybrid crimes involve both physical violence and digital asset tracing, requiring cross-border coordination and technical expertise.
- **Public confidence risk**: Violent, high-profile cases, such as kidnappings and mutilations can erode public trust in law enforcement's ability to protect cryptocurrency users.

QPS actions

- Continue to expand crypto tracing training across QPS units, using blockchain forensic analysis tools to support the growing demand for expertise in cryptocurrency enabled crime investigations
- Engage in proactive profiling of high-risk individuals and monitor online platforms for targeting behaviour to prevent further victimisation.
- Promote public awareness campaigns on operational security, especially for crypto holders.

Examples

- **Brisbane home invasion crypto theft:** In January 2025, three offenders, allegedly tied up residents and stole over $1million in cryptocurrency and cash, forcing the victim to install remote-access software to transfer assets.
- AFP Operation Gouldian[1] was a Queensland based investigation which highlighted the involvement of OCG's in obfuscating illicit profits using Bitcoin.

5. PHYSICAL WORLD OFFENDING VIA CAAS – SERIOUS CRIME/ILLICIT TOBACCO/FIREARMS

5.1 Illicit Tobacco – Use of Encrypted Devices

How it works

Queensland's illicit tobacco market continues to be operated by organised criminal networks. These groups are known to use intimidation tactics against legitimate retailers and coordinate criminal activities, including arson through encrypted messaging platforms and disposable devices. Their operations reflect a scalable CaaS model, posing a persistent threat to community safety and legitimate business.

QPS challenges

- **Encrypted communications:** Criminals use secure apps to coordinate arson and extortion, hindering interception and attribution. The veil of anonymity, provided by apps allows criminals to engage in illicit activities, making detection by law enforcement more challenging.
- **CaaS subcontracting:** Criminals outsource violent acts to gangs and youth offenders, complicating investigations and prosecutions.

[1] https://www.afp.gov.au/news-centre/media-release/bitcoin-beachside-mansion-and-mercedes-benz-qld-man-forfeits-more-45

- Serious crimes are increasingly facilitated through encrypted devices, enabling disconnected individuals to engage in purely transactional offending for financial gain—mirroring the structure and functionality of legitimate tasking apps used by the public.
- Retailer intimidation: Arson attacks have targeted tobacconists refusing to comply with criminal demands, with threats escalating to physical harm.

QPS actions

- Highly publicised operations like AFP Ironside and Kraken have demonstrated the effectiveness of combining human intelligence with technical capabilities to infiltrate encrypted platforms used by organised crime. These models offer scalable strategies for the QPS to disrupt encrypted communications in illicit tobacco networks.
- Continue to work with and strengthen multi-agency intelligence sharing to track facilitators attributed to encrypted devices and coordinate cross-border efforts.

Queensland impacts

- Over twenty (20) arson attacks linked to illicit tobacco have occurred across Queensland, including Brisbane, Mount Isa, and Townsville, since 1 January 2025, impacting the community.
- Taskforce Masher was commenced to investigate the organised crime linked to illicit tobacco, has led to multiple arrests and seizures, disrupting syndicates identified using encrypted devices to coordinate arson attacks.

5.2 Firearms – Privately Made Firearms and 3D Printing

How it works

Privately Made Firearms (PMFs), often referred to as ghost guns, are increasingly being manufactured using 3D printers and online blueprints. These weapons are unregistered, lack serial numbers, and are often indistinguishable from factory-made firearms, making them difficult to trace and regulate.

QPS challenges

- **Rapid technology adoption:** The affordability and accessibility of 3D printers and online tutorials are enabling individuals and organised crime groups to manufacture firearms at scale.
- **Blueprint proliferation:** Digital blueprints for firearms are widely available on the clearnet and darknet.
- **Organised crime involvement:** PMFs are increasingly linked to organised criminal networks in Queensland, with some weapons used in violent crimes.
- **Serious crimes:** PMFs are also being used by criminals not necessarily linked to criminal networks, to commit a range of serious offences.
- **Detection and enforcement:** PMFs are difficult to detect, easy to destroy, and often assembled using a mix of printed and conventional parts.

QPS actions

- Ongoing engagement with 3D printing industry to develop safeguards and reporting mechanisms for suspicious requests.
- QPS are conducting operations targeting persons involved in the manufacture and trafficking of PMF's using 3D printing technology.

Queensland impacts

- QPS have seized 3D-printed firearms linked to attempted murders and drug trafficking.
- NSW and Tasmania have legislated against blueprint possession.
- Experts warn that some 3D-printed firearms are now fully automatic and capable of firing 40 rounds before reloading, posing a serious threat to public safety.
- Any disconnect between law and technology would undermine enforcement efforts and exposes vulnerabilities in public safety and crime prevention.

Examples

- **Toowoomba:** In June 2025 a 3D-printed suppressor was seized during a home search (alongside multiple firearms/ammunition).
- **Maryborough:** In January 2025 an alleged use of a 3D-printed firearm in a shooting; attempted-murder charges laid.
- **Burpengary:** In January 2025 a suspected 3D-printed 'ghost gun' was located during a routine traffic stop.
- **Redbank Plains:** In September 2024, the active 3D printing production of a Harlet 22LR single shot pistol was occurring during the search of a dwelling. Evidence was gathered showing the offender was producing these to order (One (1) week handling time) and selling them for $1500 each with a $300 deposit.

6. SCAM/PHISHING-AS-A-SERVICE

6.1 The Role of SIM Boxes in Facilitating Phishing Scams

How it works

SIM boxes are devices that can house dozens to hundreds of SIM cards and send bulk short message service (SMS) messages. Organised crime groups use them to conduct large-scale phishing scams, impersonating legitimate entities to steal personal and financial information.

QPS challenges

- **Remote operation:** SIM boxes are often operated remotely by third-party mules, creating layers of separation that hinder detection and prosecution.
- **Legal ambiguity:** Possession of SIM boxes remain legal in Australia, making it difficult to prove criminal intent without direct evidence of misuse.
- **Resource-intensive investigations:** Tracking and disrupting SIM box networks requires significant technical and human resources.
- **Volume of attacks:** A single SIM box can send millions of scam messages daily, overwhelming victims.

- **Identity theft:** These scams are often registered using stolen identities, compounding victim harm.

QPS actions

- Continue to strengthen interagency collaboration through the Joint Policing Cybercrime Coordination Centre (JPC3), which has proven effective in national operations.
- Strengthen QPS capabilities to address the offending associated with the possession and use of SIM boxes for fraudulent purposes.
- Engage telcos and regulators to improve SIM registration processes and detect bulk SMS anomalies.
- Expand open source intelligence and cyber forensics to monitor SIM box activity and identify emerging scam patterns.

Queensland impacts

- In June 2024, QPS seized SIM boxes used to send over 1.7 million scam messages in a two-week period, targeting toll payment victims.
- In July 2024, Queensland participated in a national investigation that led to the seizure of 29 SIM boxes and over 500 SIM cards
- In mid-2024, QPS seized a SIM box used to send almost 5 million scam 'smishing' (SMS phishing) messages to Australian mobile numbers.

Examples

- **Gold Coast:** In May 2024, two people charged using SIM boxes to impersonate legitimate companies, stealing identity data.
- **National operation**: In July 2024, AFP and QPS-led operation disrupted multiple SIM box networks, recovering cash, luxury goods, and stolen identities.
- **Townsville**: In September 2024, one person was charged using a SIM box sending SMS phishing messages across Australia.

7. RANSOMWARE AND CYBER EXTORTION

7.1 The Role of Ransomware and Cyber Extortion in Facilitating Crime

How it works

CaaS lowers the barrier to entry: ransomware kits and phishing services are accessible to non-technical offenders, while cryptocurrencies enable ransom payments and laundering. Data-theft extortion (with or without encryption) is commonly used to pressure victims. Artificial Intelligence (AI) is already improving lure quality and scale (cleaner emails/messages/voice), making initial access harder to detect and contributing to rising tech-enabled losses in Queensland and nationally.

QPS challenges

- **Lowered barrier to entry:** Ready access to illicit tools (incl. ransomware kits/phishing services) enables more actors to offend.

- **Crypto complexity:** Pseudonymous transactions complicate tracing and recovery of ransom flows.
- **Cost/access to tooling:** AI, blockchain analytics and similar solutions are expensive, limiting affordable options.
- **Cross-border environment:** Offenders, infrastructure and payments often span jurisdictions, requiring sustained external cooperation.
- **Under/late reporting:** Many victims are reluctant to report cyber offences to police, constraining early evidence collection.

QPS actions

- **Targeted capability uplift:** Focus people/process uplift aligned to ransomware/cyber-extortion investigations.
- **Leverage technology where feasible:** Use advances in AI, blockchain analytics and data-sharing frameworks to enhance investigations and disrupt networks (subject to affordability/access).
- **Partnerships & cooperation:** Strengthen collaboration with private-sector technology firms and maintain/increase international cooperation to address cross-border elements.

Queensland impacts

- Investment and romance scams were highest-loss categories in Queensland in 2024.
- ReportCyber referrals to QPS show an upward trend across recent years; under-reporting remains an issue.
- It is highly likely AI adoption will continue to increase volume and sophistication, driving further losses.

Examples

- ACCC / National Anti-Scam Centre reporting indicates over $51 million in losses in 2024 *(investment scams around 58%; cryptocurrency common payment method)* in Queensland.
- Investment scams continue to drive the largest reported losses nationally, with cryptocurrency frequently used as the payment method.
- National Anti-Scam Centre commenced 1 July 2023 to coordinate government, law-enforcement and private-sector information against technology-facilitated scams.

8. ONLINE CHILD ABUSE

8.1 Pay-Per-View Child Abuse Content

How it works

Pay-per-view child abuse involves offenders paying facilitators to live-stream on-demand sexual abuse of children via encrypted apps or private groups. Payments are made using remittance services, e-money, cards, or cryptocurrency, often in small, repeated transfers to disguise activity. While livestreams disappear quickly, financial trails remain a key detection point.

QPS challenges

- **Cross-border and real-time offending:** Victims and facilitators are frequently based offshore; livestreams disappear quickly leaving limited content evidence (mainly logs/metadata).
- **Payment obfuscation:** Fragmented low-value payments across e-money, remitters, and virtual assets complicate detection and tracing.
- **Platform detection gaps:** eSafety's 2024 transparency findings revealed major platforms under-report livestreamed abuse and grooming, limiting data for law enforcement.
- **Rising demand:** National reports of online child sexual exploitation in Australia increased by ~41% in 2024-25, raising investigative workload.

QPS actions

- Apply AUSTRAC's financial-crime guide and FATF typologies to bank, e-money and crypto flows; use red flags to accelerate SMRs and seizures.
- Leverage QPS Argos' capability with Australian Centre to Counter Child Exploitation (ACCCE) and AFP liaison posts to fast-track victim identification and offshore disruption.
- Use eSafety transparency outcomes to press for stronger livestream detection and preservation of key data.
- Deploy the Australian Institute of Criminology's machine-learning indicators to triage suspect transactions and prioritise Queensland-linked investigations.

Queensland impacts and examples

- AFP charged a Queensland man over alleged production of child exploitation material in the Philippines, evidencing local involvement in pay-per-view abuse. QPS Argos investigators charged six Queensland men with 100+ offences for online child exploitation; evidence showed payments for livestreamed abuse.
- Demand generated locally sustains organised facilitation networks abroad, fuelling ongoing exploitation.
- Since 2022, AUSTRAC's financial crime guide and industry alerts have generated over 400 suspicious matter reports (SMRs). These referrals have directly contributed to AFP/ACCCE investigations, with the AFP reporting a 45% year-on-year increase in cases referred to state police.

8.2 Sadistic Online Exploitation

How it works

Sadistic Online Exploitation (SOE) is an escalation of sextortion where offenders coerce underage victims into producing child abuse material depicting self-mutilation, sexual assault, animal cruelty, or even live-streamed suicide. Contact often begins on open chat platforms and then shifts to encrypted services such as Discord and WhatsApp. Offenders may also operate in violent online communities that encourage sadistic content and recruit members through coercion.

QPS challenges

- Victims as young as 12 have been coerced in sadistic sextortion cases to live-stream violence and self-harm under offender direction.
- Exposure to SOE material (mutilation, suicide, animal cruelty) places frontline officers at heightened psychological risk.
- Offending is under-reported, making prevalence difficult to measure.
- Offenders exploit encrypted, mainstream platforms and are frequently interstate or overseas, limiting QPS jurisdiction and complicating disruption efforts.

QPS actions

- Standardise QPS computer system tagging to ensure SOE incidents are accurately captured.
- Use trauma-informed engagement and referral pathways to reduce victim withdrawal.
- Strengthen collaboration across Child Abuse and Sexual Crimes, Argos, Cybercrime, and partner agencies.
- Align with national prevention and disruption efforts to surface Queensland-linked victims and offenders.

Queensland impacts

- Victims in Queensland reflect wider patterns, often adolescents with mental health issues or suicidal ideation, making them highly vulnerable to coercion.

Examples

- **Queensland case study**: A 2024 QPS–NSW Police joint investigation identified a Queensland victim, under the age of 16, groomed via Emerald Chat and Discord, coerced into sexual acts and carving symbols into her skin. The male offender was arrested in NSW.
- **“Hurtcore” networks:** Investigations have linked SOE to extremist and “hurtcore” networks, including the 764 group, which forces victims to self-harm and share violent content as part of peer-driven coercion.