IFW
GLOBAL

Investigations | Intelligence | Recovery

PARLIAMENTARY JOINT COMMITTEE ON LAW ENFORCEMENT

Re-referral of inquiry into the capability of law enforcement to respond to cybercrime

This supplementary submission has been prepared to update IFW Global's evidence since our February 2024 and June 2024 filing. We attach three recent case studies demonstrating systemic gaps in state law enforcement responses to crypto-enabled fraud (Victoria and NSW), despite clear legislative powers and available freezing mechanisms.

We also highlight an AFP–JPC3 success with the Royal Thai Police in June 2025 to illustrate what effective international coordination looks like when properly resourced.

Certain annexures provided separately to this submission contain sensitive victim and investigative material; we request those be received **in confidence**.

Introduction to Case Studies

Since my previous submission to the Committee in June 2024, IFW Global has continued to investigate major fraud cases affecting Australian victims. In several matters, we provided state police with irrefutable blockchain evidence and clear pathways to secure stolen assets. Despite this, police either refused or failed to act, citing lack of authority, misunderstanding of powers, or jurisdictional limitations.

The following case studies, drawn from live investigations in Victoria and New South Wales, illustrate these systemic failures in practice. They demonstrate that existing legislation and investigative tools are available but remain underutilised, resulting in lost opportunities for asset recovery, severe harm to victims, and a growing public confidence gap in law enforcement's ability to respond to cyber-enabled fraud.

Systemic Failures in State Responses to Cyber-Enabled Fraud

These failures are not isolated incidents but part of a broader systemic pattern of incapacity, poor coordination, and a reluctance to exercise existing legislative powers.

Case Study 1 - Adam Daniels (victim)
Victoria Police Refusal Despite Clear Powers

Mr Adam Daniels, a Victorian resident, lost over AUD $520,000 in a USDT (Tether) investment fraud. He engaged IFW Global immediately after the fraud, authorising us to act on his behalf. Mr Daniels has authorised IFW Global to name him in this submission.

IFW Global traced Mr Daniels' stolen funds through HTX (Huobi) in Hong Kong, which confirmed receipt of his funds into exchange wallets. The funds were then moved to the TRON blockchain and consolidated into three wallets containing over AUD $800,000 in criminal proceeds, identified using TRM Labs forensic tools.

USDT on TRON is freezable by Tether through its T3 Financial Crime Unit (T3 FCU), which has frozen over USD $100 million in illicit assets since its creation in August 2024.

The Moorabbin CIU of Victoria Police took carriage of Mr Daniels case and commenced an investigation. Over the next few weeks, Mr Daniels attempted to introduce IFW Global to the Moorabbin CIU, but they refused to engage. IFW Global provided evidence to Detectives at Moorabbin CIU showing where Mr Daniels funds were sitting and offered to introduce Moorabbin CIU Detectives to the T3 FCU. Furthermore, IFW Global engaged with the AFP's JPC3 who provided Moorabbin CIU Detectives with the correct template for submitting a freeze request to Tether.

Despite irrefutable evidence and a simple mechanism to secure the funds, detectives at Moorabbin CIU:

- Refused to issue a freeze request, stating to Mr Daniels in an email, *"Victoria Police is not a debt collection agency."*
- Rejected engagement with IFW despite a signed letter of authority from the victim.
- Delayed taking statements, failed to provide updates, and ignored their obligations under the Confiscation Act 1997 (Vic) s31D and the Victims' Charter Act 2006 (Vic).
- Reported to Daniels that the case would take "three months" before the Cybercrime Squad reviewed it.

The AFP indicated willingness to act, yet Victoria Police declined to escalate or transfer the matter.

Mr Daniels has suffered severe psychological distress and has made a formal complaint to Tim Richardson MP, with IFW escalating a complaint to Victoria Police Professional Standards and the Victorian Minister for Police. No response has been received to date.

This case demonstrates that powers exist but are ignored, coordination with AFP fails, and victims remain unprotected even when recovery is achievable.

Case Study 2 - Andy Token Case
Victoria Police Failure to Freeze Hosted Wallets

Mr JY was the victim of a large-scale cryptocurrency theft involving the unauthorised diversion of digital assets valued at approximately USD $2 million (referred to herein as the "ANDY Token" case).

The incident occurred on or about 7 June 2024, when Mr JY's crypto holdings were illicitly transferred to external wallets without his authorisation.

Mr JY engaged IFW Global to conduct a forensic blockchain investigation. IFW Global's cyber team traced the unauthorised transactions across the blockchain, identifying multiple wallets into which the stolen ANDY Token proceeds were transferred. Transfers were tracked to at least one hosted exchange (KuCoin), creating a viable opportunity for asset preservation and recovery.

Despite the provision of comprehensive forensic evidence and ready avenues for preservation, Victoria Police failed to initiate a freezing action against the identified wallets. Officers have indicated uncertainty about their authority to act once funds reached hosted exchange environments. This hesitation contrasts with established precedent (e.g. Operation Taipan) and undermines the legislative intent of asset preservation provisions already available to police.

Operation Taipan was a Victoria Police Cybercrime Squad investigation that secured Australia's first conviction for crypto money laundering. The case demonstrated that Victoria Police had already used Tether wallet freezes to preserve digital assets linked to criminal proceeds.

As I have highlighted in the Adam Daniels case, the Confiscation Act 1997 (Vic) s31D empowers officers to seek freezing orders over digital assets suspected to be tainted property. While the Act empowers investigative officers, including police, to apply for freezing orders, it does not explicitly state that police must make such requests. The Act sets out the process for police to apply for a freezing order, not the circumstances in which police cannot exercise these powers. Thus, it seems Victoria Police may have a lot of discretion here to do as it pleases.

Mr JY suffered catastrophic financial loss, with direct implications for his personal and business affairs. He has expressed deep frustration at law enforcement's inaction, despite clear evidence and IFW Global's support in providing forensic intelligence. The lack of police intervention risks further dissipation of the stolen assets, permanently frustrating restitution efforts.

Case Study 3 – Mr DH
NSW Police Command Block Despite Proactive Detectives

Mr DH, an NSW-based victim, lost funds in a cryptocurrency fraud. IFW Global traced 3.14 BTC into unhosted wallets and provided wallet tracing and exchange data. Bondi Detectives engaged actively with exchanges, requesting disclosures and attempting to preserve evidence. Bondi detectives were described as professional and cooperative.

However, NSW Cyber Command overruled them, advising that NSW Police had no jurisdiction to seize funds from unhosted wallets.

The Cyber Command directed detectives to instruct the victim to seek a Mareva Order through civil courts. This solution breaks evidentiary continuity, making criminal prosecution of offenders near impossible. Despite detectives' efforts, senior command policy blocked recovery. The victim was left with only civil remedies, undermining the principle that fraud is a criminal matter.

Even when frontline officers are willing, command-level interpretations of jurisdiction block action. This highlights the urgent need for clear national frameworks and leadership in cyber-fraud enforcement.

Overall Findings from the Case Studies

Taken together, these cases demonstrate examples of failures where victims are left without recourse, despite laws, precedents, and technical mechanisms being available to law enforcement. The issues identified include:

1. Police declined to use provisions such as s31D of the Confiscation Act 1997 (Vic), despite their clear applicability to digital asset freezing.
2. Officers wrongly asserted that they lacked power to freeze assets once they entered hosted exchanges, contradicting both the law and precedent (e.g. Operation Taipan).
3. Frontline detectives were sometimes proactive and cooperative (as in the Mr DH case), but senior command overruled them, demonstrating a cultural problem of discretion over duty.
4. Even where the AFP JPC3 unit was willing to act, state police refused to escalate or transfer carriage, leaving cases stranded in procedural limbo.
5. Victims were directed towards civil remedies (e.g. Mareva Orders), undermining criminal prosecutions and shifting the burden onto individuals rather than treating fraud as a serious crime.
6. Beyond financial loss, victims experienced severe psychological harm, frustration, and disillusionment with law enforcement's ability to protect them.

Illustration of an Effective International Operation

AFP–JPC3 Success in Thailand

In contrast to the systemic failures outlined above, the AFP-JPC3 led collaborative success underlines what is possible with proper resourcing and global reach. In June 2025, as part of Operation Firestorm, the AFP's Joint Policing Cybercrime Coordination Centre (JPC3) partnered with the Royal Thai Police (RTP) to dismantle a highly sophisticated investment fraud syndicate operating near Bangkok, Thailand.

The joint law enforcement operation resulted in a coordinated raid on a "boiler-room" scam centre, arresting 13 individuals, including five Australians, six British nationals, a Canadian, and a South African, accused of running a bogus high-yield bond scheme targeting over 14,000 Australians, and amassing at least AUD 1.9 million in stolen funds within just two months of operation.

The AFP provided pivotal intelligence through its international network, which enabled Thai police to identify and eventually arrest the syndicate. The success of this operation demonstrates how intelligence-sharing and operational collaboration can dismantle transnational cyber-fraud networks. Assistant Commissioner Richard Chin characterised this as "*one of the most elaborate investment scam operations*" encountered by the AFP. Reflecting on broader trends, the AFP highlighted Southeast Asia's rising prominence as a region for scam centre operations and referenced prior successful takedowns in Manila as part of the same coordinated effort.

Why This Matters

The Thailand operation is a compelling model of success, irrefutable proof that when AFP is empowered with resources and global partnerships, it can achieve meaningful outcomes. It underscores that cyber-enabled fraud is not a local phenomenon but a serious borderless crime that is growing exponentially year after year. Without similar coordination in every region and scale, criminals will continue exploiting jurisdictional gaps.

The success also highlights the necessity for increased staffing for AFP JPC3, particularly overseas liaison officers, investigators and intelligence analysts. The JPC3 should have sustained operational funding, including covert surveillance and cross-border coordination capabilities.

Recommendations & Conclusion

- Establish a dedicated federal cyber-fraud taskforce with international mandate.
- Introduce mandatory referral protocols from state police to AFP JPC3.
- Require training in crypto tracing and freezing at both state and federal levels.
- Create KPIs on victim restitution for law enforcement agencies.
- Expand AFP JPC3 resources, including overseas liaison posts and operational funding.

It is my view that Australia's current law enforcement framework is incapable of responding effectively to cyber-enabled fraud. Laws and mechanisms exist, but police discretion, poor training, and interagency failures prevent their use. Without a dedicated federal cyber-fraud taskforce, national training, and mandatory referral protocols, victims will continue to suffer while billions in traceable criminal proceeds remain unrecovered.

Ken Gamble
Executive Chairman
IFW Global
3 September 2025