IFW
GLOBAL

Investigations | Intelligence | Recovery

Further Submission to the Parliamentary Joint Committee on Law Enforcement in response to Questions on Notice, 23 May 2024

12 June 2024

Dear Committee Members,

I appreciate the opportunity to offer additional recommendations aimed at enhancing the capabilities of Australian law enforcement in combating cybercrime, with a specific focus on transnational cyber-enabled investment fraud that targets Australian citizens. As discussed in my previous testimony and submission, this is a rapidly growing threat that requires urgent action to protect Australian citizens and the economy.

The specific areas I was asked to address further were:

1. What additional resources are needed by law enforcement, particularly the Joint Policing Cybercrime Coordination Centre (JPC3), to address the increasing threat of cyber-fraud? *The committee is seeking evidence on the current capacity of law enforcement and what resourcing would look like.*
2. What type of education and training is still needed by law enforcement to combat cyber-fraud? *The committee noted that all states, except for Tasmania and the Northern Territory, currently have officers based in JPC3, and collaboration between state policing and the AFP is on a stronger footing.*

Current Limitations of the JPC3

The Joint Policing Cybercrime Coordination Centre (JPC3) is an important initiative set up with the intention to "aggressively target cyber threats, shut them down, and bring offenders to justice" using "far-reaching Commonwealth legislation and high-end technical capabilities".

These statements suggest a more proactive and intensive approach to cybercrime investigations than has previously been the case but there is no reference to how JPC3 intends to deal with a multibillion-dollar cyber-fraud problem across Australia.

The JPC3 currently lacks the capacity and capabilities to effectively deal with the sheer volume and complexity of highly organised cyber-fraud targeting Australians.

As a coordination centre, it relies on the resources and priorities of the participating agencies, which are often stretched thin or focused on other aspects of cybercrime and not cyber-fraud.

In particular, the JPC3 does not have the dedicated resources to develop the deep international intelligence networks needed to identify and track the overseas organised cyber-fraud groups behind most of the sophisticated investment frauds hitting Australian victims and causing financial devastation.

Cyber-fraud is now widely known to be linked to Transnational Serious and Organised Crime groups (TSOC) involved in all other forms of organised crime including money laundering, drug trafficking, human trafficking, terrorism financing, illegal weapons, corruption, computer hacking and intellectual property theft.

Building the intelligence capabilities to combat cyber-fraud requires persistent effort, specialist skills, and close partnerships with foreign law enforcement and private sector actors in key cyber-fraud hotspots around the world.

The AFP's Cybercrime Division, as the federal law enforcement lead, has its resources largely committed to responding to major cyber incidents like systems intrusions, ransomware attacks, and critical infrastructure threats. While important, this focus on cyber-attacks and cyber security issues means that cyber-enabled fraud, especially against individuals, is not receiving the attention it deserves as this is by far the biggest cybercrime threat facing Australians in terms of financial losses in the billions of dollars.

Compounding this, the AFP's mandate essentially precludes it from investigating cyber-enabled investment frauds against individuals, even when the losses are in the millions per victim.

The AFP maintains this is a matter for state police to investigate complaints of serious fraud online, while the state police often lack the technical skills, resources and international reach to effectively tackle sophisticated global cyber-fraud syndicates. Fragmented responsibility and barriers to information sharing between agencies further hamper the law enforcement response.

If law enforcement agencies genuinely want to foster productive collaboration, they must facilitate and encourage interactions among frontline staff. For example, collaboration among officers of the same rank or frontline investigators in law enforcement agencies, such as ASIC (Australian Securities and Investments Commission) and the AFP (Australian Federal Police).

When collaboration only occurs at the leadership level, it can lead to problematic situations, such as the current issue at ASIC regarding the 34,000 Australian victims identified in Serbia by the German Police that were never contacted or alerted by any authorities in Australia. This case implies that without proper collaboration at the frontline level, important information may not be shared effectively, leading to mishandling of cases or data.

In my extensive experience in these types of international cases, interactions between frontline detectives or investigators tend to be the most productive, effective and reliable forms of collaboration.

Without this important collaboration, the result is a huge gap in Australia's defences against serious organised cyber fraud, leaving Australians uniquely exposed among Western nations.

AFP Resources

To close this gap, the AFP urgently needs a substantially higher level of dedicated funding and specialised resources to establish a standing capability to combat international cyber-enabled fraud and identify the crime bosses behind it.

This should include a core group of experienced criminal investigators and intelligence analysts trained in the latest cyber investigative techniques, cryptocurrency tracing, covert engagement and international money laundering methods.

They should be supported with the technical tools, operational budgets and high-level mandates to pursue cases across the globe in partnership with international law enforcement and, where necessary, private sector experts and professionals.

Additionally, more training and resources are needed for state police cybercrime units to boost their ability to investigate the onshore elements of international cyber-frauds and provide complementary state-level support to federal efforts.

Only by making cyber fraud an urgent cross-jurisdictional law enforcement priority and allocating the resources and international capabilities to match, can Australia then begin to turn the tide on the growing scourge of cyber-fraud.

Building these capabilities will take time and money, but failing to do so will only lead to more Australians falling victim and more criminal syndicates viewing Australia as a lucrative target.

To enhance state and federal law enforcement capabilities in detecting, investigating and prosecuting cyber-fraud, I recommend the following key measures:

Cyber-fraud Taskforce

1. Establish a dedicated, intelligence-driven federal cyber-fraud taskforce focused on proactively identifying and dismantling the global criminal syndicates behind cyber-enabled investment fraud. This taskforce should be:

    - Adequately resourced to fund overseas travel and extraditions, engage expert legal and technical support including from the private sector, and develop efficient and up-to-date intelligence capabilities.
    - Empowered with a clear mandate to pursue the fraud kingpins in their overseas locations, not just local money mules, and to collaborate closely

with foreign law enforcement, anti-cybercrime and anti-corruption agencies, to arrest and extradite offenders.
- Supported by specialist investigators, prosecutors and legal experts in cyber forensics, cryptocurrency tracing, and international financial investigations.

Cyber-fraud Training

2. Provide enhanced cyber-fraud training for law enforcement officers at all levels, including:

    - Incorporating fraud and cyber-fraud fundamentals into basic training for all state and federal police.
    - Developing a national centre of expertise to train officers in cutting-edge cyber investigative techniques, cryptocurrency tracing, and digital forensics.
    - Creating a cyber-fraud investigations specialisation track for detectives, covering syndicate operations, money laundering typologies, intelligence gathering, and legal aspects.
    - Delivering awareness training to all public-facing officers on prevalent cyber-enabled frauds and referral mechanisms.

Public-Private Collaboration

3. Foster active collaboration and intelligence sharing on cybercrime threats between law enforcement, industry, and the private sector by:

    - Establishing formal MoU's and public-private partnerships with vetted private investigation, forensic, financial and intelligence firms that have the global networks and expertise to provide actionable leads.
    - Sharing strategic threat intelligence between state, federal and international law enforcement agencies in a timely manner.
    - Working with banks and cryptocurrency exchanges to improve suspicious activity reporting and simplify information sharing processes.
    - Collaboration with domestic and overseas agencies and judicial authorities to extradite offenders and identify and freeze assets to facilitate the return of stolen funds.

Legislative Framework

4. Bolster the legislative framework and police KPIs to prioritise cyber-fraud:

    - Consider legislative reform to incentivise asset recovery and restitution to the victims.
    - Include cyber-enabled fraud in the KPIs and performance metrics for law enforcement.
    - Ensure law enforcement has adequate powers to compel information from cryptocurrency exchanges and digital asset service providers
    - Audit all agencies on their relevant capabilities.

Resourcing Requirements

In terms of specific resourcing requirements, it is difficult to estimate precise numbers without access to law enforcement budgets and staffing levels. However, successfully standing up dedicated cyber-enabled fraud taskforces will likely require dozens of additional specialist officers, investigators and analysts at the state and federal levels, supported by enhanced technical capabilities and operational budgets in the millions of dollars.

Training and equipping the broader law enforcement community to better handle cybercrime cases will also require significant investment.

While these resource needs may seem substantial, they must be weighed against the billions of dollars in losses currently suffered by Australians each year to cyber-enabled fraud, much of which is not being adequately addressed under current law enforcement arrangements and priorities. Proactive investment now in cybercrime fighting capabilities will pay dividends down the road.

The new Australian Cyber Security Strategy and other strategic reforms are positive steps, but still leave gaps in addressing cyber-enabled fraud from an offensive, crime-fighting perspective. Cybersecurity and cybercrime are distinct issues requiring different approaches.

By providing law enforcement with the tools, training and mandate to proactively tackle cyber-enabled fraud, Australia can become a global leader in combating this transnational threat rather than an attractive target.

I appreciate the Committee's consideration of these recommendations.

Sincerely,

Ken Gamble
Executive Chairman
IFW Global Investigations Pty Ltd

Contributor: **Mark Solomons**, Senior Investigator, IFW Global