15 July 2024

Committee Secretary
Parliamentary Joint Committee on Law Enforcement
PO Box 6100
Parliament House
Canberra ACT 2600

By email: le.committee@aph.gov.au

Australian Payments Network (AusPayNet) welcomes the invitation to make a submission to the Parliamentary Joint Committee on Law Enforcement's inquiry into the capability of law enforcement to respond to cybercrime.

AusPayNet is the industry association and self-regulatory body for the Australian payments industry. We manage and develop standards and guidelines governing payments in Australia. Our purpose is to create confidence in payments by: setting enforceable industry standards for a safe, reliable and effective payments system; leading transformation in payments to drive efficiency, innovation and choice; and being the home for ecosystem collaboration and strategic insight. AusPayNet currently has more than 150 members including financial institutions, payment system operators, major retailers and financial technology companies.

Introduction

The growing prevalence of cybercrime poses a significant national threat, generating serious economic and social harms across Australia. AusPayNet therefore welcomes the Committee's inquiry into the capability of law enforcement to respond to cybercrime, to help ensure that Australian authorities are well equipped and appropriately enabled to reduce and address the consequences of these crimes.

AusPayNet recognises the important role of law enforcement in combatting cybercrime. We also acknowledge the ongoing work of the Government and other regulators in enhancing the country's defences again all forms of cyber-enabled crime. This includes the formation of the National Anti-Scam Centre (NASC), the planned introduction of industry scam codes, the release of the Australian Cyber Security Strategy, and ongoing participation in numerous public-private initiatives on cybercrime. However, as the frequency and complexity of cybercrime continues to increase, ongoing improvements in Australia's capabilities to respond to these crimes – particularly by law enforcement agencies – will be critical. In particular, enhanced public-private, cross-agency, and cross-border collaboration will become increasingly important in the country's response efforts.

Over the past decade, AusPayNet has worked closely with members, Government, law enforcement, and other stakeholders on a range of initiatives to help defend the payments ecosystem and its users against economic crime. We understand that the Committee has already received extensive evidence from a range of stakeholders on the key issues being examined through this inquiry. This submission will focus on the areas in which AusPayNet has gained particular insights through our work with law enforcement and payments system participants. Given AusPayNet's remit and expertise, the submission will focus on the key challenges and opportunities for law enforcement in countering cyber-enabled economic crime, and particularly online scams, fraud and money laundering.

Please note that the views expressed in this submission are those of AusPayNet Management, and may not necessarily represent the views of each of our members.

AusPayNet's role in mitigating cyber-enabled economic crime

As part of our strategic priorities, AusPayNet is committed to working with members, Government, law enforcement, and other stakeholders to help defend the payments system and its users against economic crime. One of our key initiatives in this space is leading the cross-sectoral Economic Crime Forum (ECF). The ECF brings together a wide range of stakeholders – including law enforcement and intelligence agencies, regulators, AusPayNet members (primarily banks in this instance), and various industry bodies – to share intelligence on emerging threats and collaborate on joint responses and tactical initiatives to help prevent, detect and disrupt economic crime.[1]

The ECF has become the public-private information channel for several law enforcement task forces, including Operation Themis (which targets serious financial crime), Operation Helios (targeting cybercrime), and Operation Kubera (targeting money laundering). The ECF has also established a joint industry and law enforcement working group for delivering operational intelligence packages to the Joint Policing Cybercrime Coordination Centre (JPC3), the National Anti-Scam Centre (NASC) and other law enforcement agencies.

Insights on law enforcement's capabilities in responding to cybercrime

Public-private and cross-agency partnerships

The work of the ECF to date highlights the value of public-private partnerships for enhancing law enforcement's ability to detect and respond to cybercrime. Such partnerships allow law enforcement to leverage private sector intelligence, expertise, and technical capabilities to supplement their own core competencies in investigation and prosecution. These synergies are especially important for high-volume and increasingly sophisticated offences such as cybercrime. The growing complexity of cyber-enabled economic crime in particular – which often involves rapidly moving funds through multiple financial institutions and payment networks to avoid detection – means that siloed approaches to the detection and prevention of such criminal activity are becoming increasingly ineffective.

Continued close collaboration between law enforcement and other regulatory and Government agencies is also important. Responsibility for addressing cybercrime in Australia currently spans across numerous regulatory bodies and law enforcement agencies at the federal, state and territory levels. Without an overarching national strategy, each of these agencies determines their own priorities and approaches to addressing their respective areas of responsibility. Cross-agency collaboration enables better exchange of intelligence, which is critical given the non-linear and interconnected nature of cyber-enabled crime. Collaboration and coordination also allow for better sharing of best practice approaches, to help uplift capabilities in responding to cybercrime across all law enforcement agencies (and other stakeholders).

[1] More information on the ECF can be found here: *The Economic Crime Forum*

AusPayNet notes that there is already widespread recognition of the value of collaboration in the fight against cybercrime among law enforcement, regulators, and Government. In addition to the ECF, initiatives such as JPC3, NASC, the Australian Cyber Security Centre (ACSC), Fintel Alliance, Serious Financial Crime Taskforce, and the industry-led Australian Financial Crimes Exchange (AFCX) have all shown the value of public-private partnerships and cross-agency collaboration to address various forms of economic crime.

As highlighted in other submissions to the inquiry, information sharing is a particularly essential element of such partnerships, providing law enforcement with quality intelligence leads across all areas of cyber-enabled crime. We therefore encourage the Government and regulators to continue prioritising the removal of any barriers to appropriate coordination and collaboration in this space (including as discussed below). Care must also be taken to prevent any potential fragmentation or inefficient duplication across different partnership initiatives.

More broadly, AusPayNet considers that – similar to the Australian Cyber Security Strategy – there may be benefit in adopting a national economic crime strategy. Implementing a unified strategy across all forms of economic crime could strengthen Australia's resilience against such crimes by establishing clear national policy objectives and priorities, assisting coordination and collaboration efforts, and leveraging the strengths of diverse stakeholders across law enforcement, Government, and private sector organisations. We note the UK Economic Crime Plan as a notable example of a national shift towards a more comprehensive, coordinated, multi-stakeholder approach to combating economic crime, rather than relying on fragmented efforts across siloed agencies and sectors.

International collaboration

As highlighted in other submissions to the inquiry, a key challenge for law enforcement is that many criminal syndicates are located offshore, increasing the difficulty of investigation and response to cybercrime due to inter-jurisdictional barriers.

The 2023-2030 Australian Cyber Security Strategy recognised the importance of global collaboration for the prevention and disruption of cybercrime. AusPayNet welcomes the Government's commitments in the Strategy to continue driving global cooperation efforts, including through close collaboration with the Five Eyes alliance and international law enforcement partners, and the establishment of regional capabilities to fight cybercrime. It will be important to ensure that Australian law enforcement agencies have the strategic mandate, resources and capabilities to develop and build upon these global partnerships.

We also recognise that there may be some key legal barriers across jurisdictions – such as bank secrecy laws – that could limit the potential for cross-border investigation, funds tracing and repatriation. Existing international cooperation forums, such as the G20, could provide a useful platform to review how international banking regulations affect criminal investigation and funds recovery efforts, and discuss options for potential legal and policy reforms that would enable safe and effective international cooperation on responding to the risks and impact of cybercrime.

Data quality and availability

Another key issue that appears to be impeding law enforcement's ability to effectively detect and respond to cybercrime is the fragmentation and inaccuracy of information available to it. Most notably, there are numerous reporting portals available for victims of cyber-enabled scams and fraud, operated by different regulatory agencies and using different terminology and definitions.[2] This can create inconsistencies in reported information, duplicate operational effort, and hinder authorities' ability to obtain an accurate view of trends and efficiently allocate resources in response to criminal activity. This is compounded by the fact that many victims are likely to only seek assistance through their bank or not report at all, which can lead to reduced detection and understanding of lower-value cybercrime.

The Financial Action Task Force (FATF) has noted that facilitating victim reporting through streamlined platforms and central repositories could enhance the detection and prevention of economic crime.[3] We understand that the ACCC is currently developing a 'no wrong door' approach for scams reporting, under which victims would still have the option to report across multiple agencies, but the information would be de-duplicated and shared with relevant government and industry bodies. While this should reduce some data quality and availability issues, it will not eliminate the potential confusion faced by victims, who would still have multiple reporting channels to choose from. While we recognise that this will require a larger upfront investment and greater cross-sectoral cooperation, streamlining all cybercrime reporting channels into a *'one door'* approach instead would likely have a much more significant positive impact on the victim's journey and experience.

A related reporting matter worth raising is the effectiveness of the suspicious matter reports (SMR) process. SMRs – which financial institutions need to submit to AUSTRAC if they suspect a customer or transaction is linked to a crime – are an important means of establishing intelligence leads for law enforcement or to support ongoing investigations. Our recent discussions with members have highlighted that while reporting entities are mandated to submit SMRs, the large volume of these reports means that a significant share is unlikely to be investigated or acted upon. The Government's proposed reforms to the AML/CTF regime are likely to lead to a further increase in SMR reporting across the ecosystem. It will therefore be important to ensure that AUSTRAC has the necessary resources to effectively analyse these and disseminate actionable intelligence to the relevant law enforcement agencies.

Intercepting and recouping proceeds of cybercrime

In Australia, the tracing, interception and repatriation of criminal proceeds is primarily carried out by financial institutions, rather than by law enforcement agencies. With most cybercrime involving a financial element, this again highlights the important of partnerships and effective information sharing between law enforcement and payments system participants for enabling the effective disruption of such activity.

Operation Dolos is one example of an initiative under which law enforcement agencies have taken a more direct role in disrupting, tracing and recovering losses from business email compromise scams. Since 2020, the taskforce – which still works closely with the financial sector – has returned over $65 million to victims of such scams.[4] Similar public-private collaboration on other types of cyber-enabled economic crime could yield similar benefits, particularly when funds have been laundered

[2] In addition to law enforcement agencies and their own bank, the following reporting channels are also currently available to victims of scams and fraud: ReportCyber (all cyber-enabled crimes), Scamwatch, ASIC (investment-related scams), the Australian Taxation Office (tax-related scams), the Australian Communications and Media Authority (telecommunications-related scams) and IDCare (for victim support). Money laundering matters can also be reported to AUSTRAC.

[3] FATF (2023), *Illicit Financial Flows from Cyber-Enabled Fraud*, November.

[4] Australian Federal Police (2024), *Commissioner Kershaw Welcomes Reappointment*, 10 May.

offshore or via a cryptocurrency exchange. We also note that Singapore has adopted a law enforcement-driven model for tracing and recouping funds lost to scams. However, increased involvement in funds tracing and repatriation would require significant – and potentially unnecessary, given industry capabilities – resource uplift across Australian law enforcement agencies.

An important industry development in this space is the establishment of the AFCX Fraud Reporting Exchange (FRX) in 2023. Historically, funds tracing and repatriation across the banking and payments ecosystem relied on bilateral communication, primarily via email and phone requests. The FRX now provides a platform for financial institutions and other participants to securely and efficiently share information on fraudulent payments in near-real time, to assist with loss prevention and recovery efforts. Under the Scam-Safe Accord, all Australian Banking Association and Customer Owned Banking Association members will join the FRX by mid-2025. Importantly, several cryptocurrency exchanges have also joined the FRX, enabling direct communication and collaboration with banks on tracing and recouping fraudulent funds transferred to those exchanges. Law enforcement and regulatory agencies have been encouraged to join the AFCX to facilitate data sharing and joint activities in response to fraud.

It should be noted, however, that with criminals taking advantage of real-time payment rails for laundering funds, the ability to intercept and recoup funds in many cases of cybercrime is limited. Many banks are now implementing risk-based frictions for certain payments in an attempt to reduce losses to cyber-enabled crimes, such as payment holds or limits for certain transactions, and customer warnings during the payment process. Efficient and timely cross-sectoral information sharing will help realise the benefits of these added frictions. Nonetheless, many high-value scams, such as investment and romance scams, are often not identified until well after the payments have been made. By this time, the funds have usually been laundered via multiple mule accounts and often sent offshore or via a crypto exchange, making them much harder to recuperate (highlighting the importance of enhancing international collaboration in this area, as discussed above).

Conclusion

AusPayNet appreciates the opportunity to respond to the Parliamentary Joint Committee on Law Enforcement's inquiry into the capability of law enforcement to respond to cybercrime. Given our role as the payments industry association, and our strategic commitment to supporting the reduction of economic crime in Australia, AusPayNet welcomes the opportunity to continue engaging with the Committee as it progresses this work. Please contact Jennifer Le, Head of Government and Regulatory Relations ([redacted]) if you have any further questions.

Yours sincerely,

[redacted]

Rajat Jain
Chief Strategy Officer
Australian Payments Network