8 August 2024

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

Submission to Inquiry: **The Capability of Law Enforcement to Respond to Money Laundering and Financial Crime**

Thank you for the opportunity to make this submission to the Joint Committee on Law Enforcement Inquiry into the Capability of law enforcement to respond to money laundering and financial crime.

This submission focuses on three key areas:

- Industry engagement
- Intelligence-led partnering, and
- Reducing barriers to share information.

I am a thought leader on anti-financial crime, currently working in the application of artificial intelligence to prevent financial crime, and with a background in financial services, international regulation, financial intelligence and law enforcement.

I look forward to further assisting the Committee.

Craig Robertson

https://www.linkedin.com/in/craig-robertson-brisbane/

Background

On 19 June 2024, the Parliamentary Joint Committee on Law Enforcement ('the Committee') agreed to inquire into and report on the capability of law enforcement to respond to money laundering and financial crime. The specific areas of enquiry for the Committee are:

a) the scale and forms of money laundering and financial crime in Australia, including their effect on the community and the economy, the types of criminal activities they fund, the methods employed by serious and organised crime, and emerging trends and threats;
b) Australia's anti-money laundering and counter-terrorism financing (AML/CTF) legislation as well as comparison with other jurisdictions and the international standards set by the Financial Action Task Force;
c) proposed 'tranche two' reforms to extend the existing AML/CTF legislation to services provided by lawyers, accountants, trust and company service providers, real estate agents and dealers in precious metals and stones and implications for law enforcement;
d) whether existing criminal offences and law enforcement powers and capabilities are appropriate to counter money laundering, including challenges and opportunities for law enforcement, such as those relating to emerging technologies;
e) the effectiveness of collaboration, coordination and information sharing between Commonwealth agencies, including law enforcement, and with authorities in other jurisdictions and the private sector;
f) the role and response of businesses and other private sector organisations, including their level of awareness, assistance to law enforcement, and initiatives to counter this crime;
g) the operation of unexplained wealth and asset recovery legislation, the Criminal Assets Confiscation Taskforce, and the Confiscated Assets Account; and
h) any related matters.

Combating money laundering threats in Australia – industry engagement

Over the last ten years, the laundering of cash through casinos and the banking system have been highly visible money laundering methods in Australia. Successful law enforcement investigations, regulatory action and media coverage have drawn attention to how criminals have exploited these sectors to launder the proceeds of crime. As criminals adapt to arrests, asset seizures and investigation techniques, understanding changes to the flows of illicit wealth in Australian must be a priority for the Australian criminal intelligence and law enforcement community.

The recent Avarus Nightwolf case provided insights to a large-scale money laundering syndicate purchasing commercial and residential property.[1] Laundering of funds through the purchase of Australian property enables criminal groups to legitimise illicit proceeds in ways that can be difficult to identify through standard detection processes used in banking and law enforcement.

To keep pace with the methods used to place and integrate illicit funds, criminal intelligence and law enforcement agencies will need to engage with a growing number of industry partners, to draw on their expertise and to collect relevant data. In terms of property, this includes real estate agents, conveyancers,

[1] 'AFP restrains $1 billion in criminal assets in major milestone,' AFP media release, 12 December 2023.

state/territory property registries and the PEXA settlement platform that settles approximately 88% of Australian property purchases[2].

Proposed anti-money laundering (AML) reforms – so-called "tranche two" – will bring some of these entities into the AML framework to play a key role in facilitating the exchange of financial intelligence with criminal intelligence and law enforcement agencies. As such, the implementation of tranche two should be seen as an opportunity by Government to harness key domain knowledge in this area – especially to understand how criminal groups may exploit the types of services, related money flows and other processes to enable money laundering.

This same concept will apply to other proposed sectors included in the AML reforms, for example, solicitors, accountants and company service providers – who also can assist criminal intelligence and law enforcement agencies with key domain expertise and insights on potential vulnerabilities that criminal groups may exploit to launder the proceeds of crime.

RECOMMENDATION 1: Use the implementation of tranche two as an opportunity to build a comprehensive picture of money laundering in the Australian property sector through investigation, research and intelligence collection by engaging in partnerships with proposed new reporting entity sectors.

Intelligence-led, not compliance-led – partnering to succeed in AML

The proposed tranche two reforms, including the expansion of sectors covered under the AML framework, has the potential to improve the quality of financial intelligence available to criminal intelligence and law enforcement agencies to counter money laundering in Australia. A key to success is the awareness in the sectors of what type of information can assist law enforcement efforts to understand, disrupt and prevent criminal activity. Government agencies involved in financial intelligence and financial investigation need to take steps to ensure these sectors are informed about existing and emerging financial crime risks to their businesses. The proposed implementation of tranche two provides an opportunity to engage affected sectors in intelligence outcomes from the outset. This can be done through:

- Education and training of tranche two businesses in financial crime risks relevant to their sectors;
- Proactive provision of feedback to new reporting entities on the quality and intelligence value of their reporting; and
- Participation of tranche two reporting entities in public-private partnerships to prevent fraud and financial crime.

Without these partnerships, there is a risk that new reporting entity sectors will focus on technical compliance with AML laws at the expense of providing quality financial intelligence and better understanding the risks of money laundering. That would represent a missed opportunity.

[2] 'Pexa Annual Report 2023', p.18.

In the United Kingdom, analysis of the reporting of suspicious activity under their AML regime indicates that suspicious reporting is still highly concentrated in the banking sector.[3] This indicates limited engagement from industry beyond financial services as key providers of intelligence. Further, the Financial Action Task Force (FATF) has also expressed concerns about the very limited scale of suspicious activity reporting from lawyers, accountants and trust and company service providers (TCSPs).[4]

Reporting of suspicious matters is only one aspect of the AML framework - but it is an important one. It would be a poor return on the investment required to implement tranche two if in five years' time suspicious matter reporting from Australian tranche two sectors was insufficient or inadequate as a result of a focus on technical compliance, not risk detection.

RECOMMENDATION 2: Actively engage the 'tranche two' reporting entity sector through case studies, monitoring and feedback on suspicious matter reporting quality and participation in public-private intelligence sharing initiatives.

Reducing barriers to collaboration and information sharing

Enabling legislation

Some of Australia's international peers have invested in building capabilities for sharing information to detect financial crime - for example, Singapore's COSMIC platform[5] and the Netherlands TMNL utility.[6] These projects have differing objectives and design features, but they have in common a voluntary information-sharing program supported by legislation which protects participating private sector organisations from liability for contractual, confidentiality and privacy breaches when sharing information for a permitted purpose. Australia lacks such provisions, leaving private sector organisations exposed to these risks, and this is a barrier to information-sharing initiatives.

These types of initiatives would support partnering, a focus on risk detection and producing insights from sectors proposed to come into the AML framework, to assist law enforcement continue to gather intelligence to counter money laundering in Australia.

RECOMMENDATION 3: Support voluntary information-sharing through legislative provisions which appropriately protect private sector entities from civil liability where they voluntarily share information as part of a public-private partnership to prevent financial crime.

Connecting scam, fraud and AML intelligence

Another barrier to effective collaboration is the divide between fraud and anti-money laundering practice in government and the private sector. Historically, banks have built anti-fraud functions to protect customer deposits and prevent losses. They have developed methods and processes, adopted

[3] SARs Annual Statistical Report 2023, UK Financial Intelligence Unit, p.7.
[4] United Kingdom Mutual Evaluation Report, Financial Action Task Force, December 2018, p.120.
[5] COSMIC, Monetary Authority of Singapore, accessed at 6 August 2024.
[6] TMNL in brief, Transaction Monitoring Netherlands, accessed at 6 August 2024.

technologies and built relationships with law enforcement to achieve this. Scam detection and prevention is generally the responsibility of fraud functions. AML functions, by contrast, have developed in response to government regulation, with the objectives of managing risk and detecting and reporting financial crime. Fraud and AML disciplines operate quite differently and are functionally separate in many financial institutions.

As we move into the era of information-sharing, government should be mindful of this split, and the costs of replicating it in public-private initiatives. These initiatives will be much more effective if they are guided by an awareness of the interplay between fraud and financial crime and a holistic approach to preventing and detecting them.

There are positive signs of this happening. For example, the National Anti-Scams Centre (NASC) is using the established Australian Financial Crime Exchange (AFCX) platform for its scams intelligence loop.[7] However, the establishment of the NASC does embed a tripartite approach, with semi-independent programs of work for fraud (AFCX), scams (NASC) and financial crime (Fintel Alliance). The AFP-led Joint Policing Cybercrime Coordination Centre (JPC3) is a fourth public-private intelligence and enforcement initiative targeting cybercrime.

In practice, there is substantial overlap between these internet-enabled, technology-driven crime types; the boundaries between them are porous. The famous Bank of Bangladesh SWIFT hack of 2016[8] shows how a criminal group can employ hacking methods to infiltrate a network and then perpetrate a fraud before laundering the proceeds. Another example is the creation of 'mule' accounts; a crucial enabler for the laundering of fraud proceeds which can be tackled through the customer due diligence measures required under AML/CTF laws.

If public-private initiatives proliferate, and intelligence is not shared between them, they will be less effective. Intelligence practitioners and investigators will always collaborate and share information informally. However, with this many initiatives focusing on internet-enabled, profit-driven crimes, government needs to play a coordinating role so that insights and methods developed in one practice group are accessible to all. This will avoid the operational siloing common in law enforcement which keeps practitioners several steps behind the criminals.

A common theme in law enforcement is the limitation of the investigate-and-prosecute model for preventing fraud and money laundering. One of the most important things private sector and government organisations can to do prevent financial crime is to uplift controls and create barriers to reduce criminal misuse of financial products and related services.

As an example of an approach, the European *barrier model* involves identifying the steps criminals need to take to commit a crime, determine the barriers which would prevent it, and then use industry-government partnerships to put those barriers in place.[9]

The AFCX, NASC, Fintel Alliance, JPC3 and other public-private partnerships will collectively help identify what barriers to financial crime Australia needs, but only if there is a conscious whole-of-government effort to extract those learnings and apply them. This may involve government agencies outside the law enforcement community, and businesses outside financial services. Engaging telecommunications and social media providers is a step in the right direction.

---

[7] 'Press conference on the expansion of the AFCX scams intelligence loop,' Australian Bankers Association, 13 June 2024.
[8] 'The Billion-dollar bank job,' New York Times, May 3 2018.
[9] 'Barrier model,' European Network on the Administrative Approach tackling serious and organised crime,' accessed at 8 August 2024.

Sustained, strategic thinking about barriers, cross-departmental coordination and willingness to engage non-traditional partners, will ensure that public-private initiatives are effective.

RECOMMENDATION 4: Facilitate the sharing of operational and intelligence insights across public-private partnerships to ensure that government and industry build a comprehensive, current picture of internet-enabled, technology-driven financial crime. Use insights about weaknesses in the control environment to create barriers across industry and government that prevent financial crime.