Opening Address to the Parliamentary Inquiry

Chair Senator Helen Polley, Members of the Committee, thank you for the opportunity to speak today.

The Australian Institute of Criminology estimates the cost of serious organised crime is above $80Billion – that Is close to double the GDP of Tasmania. Australia stands at a critical juncture in its fight against financial crime. The landscape is evolving rapidly, driven by two powerful forces: Part of its growth is due to the rise new technological innovations such as crypto and AI that creating new money laundering opportunities. A second important change is the new AML/CTF legislation that will expand the number of reporting entities to AUSTRAC will rise from 17,000 to over 100,000 that will create an information tsunami. Together, these forces are reshaping both the nature of financial crime and the challenges faced by law enforcement to conduct effective investigation.

First, the big picture.

Financial crime is evolving quickly. For example, a traditional focus of anti-money laundering regulation is the focus on large suspicious transactions as reporting entities must submit Threshold Transaction Report (TTR) for any cash transactions of $10,000 or more. Today, criminal networks are leveraging crypto currency and AI to automate and scale illicit activities. We are seeing the emergence of micro-laundering, where proceeds are fragmented into thousands of small, seemingly innocuous transactions across multiple platforms. Crypto and AI technology enables this by identifying weak points in compliance systems and exploiting them at speed and scale. Combined with deepfake technology, synthetic identities, and algorithmic obfuscation, these developments make detection exponentially harder.

At the same time, the extension of AML/CTF obligations to new sectors (lawyers, accountants, real estate agents) will dramatically increase the volume of suspicious matter reports flowing to AUSTRAC and law enforcement. While this is essential for closing intelligence gaps, it creates a data tsunami.

In the face of these challenges, Australia needs a national strategy to effectively counter financial crime threats, including enhancing law enforcement capabilities now and into the future.

Our submission offers four key recommendations to enhance law enforcement capability:

1.   Improve the quality of data and reduce false reporting.

Law enforcement agencies should be funded and required to share appropriate data with reporting entities to enable risk assessments that are evidence-based. They should also work with industry to correct risk misestimations and ensure control measures are proportionate. This will reduce unnecessary reporting and improve intelligence quality. A start has been made by the National Risk Assessment. My colleague Professor Louis De Koker will discuss this.

2.   Develop public–private partnerships and address the skills gap.

Australia faces a critical shortage of professionals trained in financial crime investigation. We recommend a national skills audit to identify gaps and inform training programs across law enforcement, regulators, and financial institutions. Based on Griffith University's assessment in developing the recently launched Master of Financial Crime Investigation and Compliance, the skills relevant for detecting, investigating and reporting financial crime are complex and interdisciplinary in nature and are drawn from several different academic disciplines, including criminology, forensic accounting and IT. Universities can play a pivotal role in creating career pathways and delivering specialised education to law enforcement and the organisations law enforcement work with.

Universities can also play a pivotal role in delivering specialised research that enhances law enforcement capabilities. In the UK the National Economic Crime Centre have published "The Areas of Research Interest (ARI)" summarises the

key areas where the National Economic Crime Centre and the Home Office would welcome further research on economic crime over the next 3 years. This is a great example of how Universities can conduct research to support law enforcement capability - but this requires an increase in the amount of data available to do so. Currently, research is limited, and no program exists to support this – unlike the national security research coordinated by Office of National Intelligence. A similar approach specific to law enforcement to counter organised crime, in particular financial crime, would see advancements made through research and innovation driven out through partnerships between universities and law enforcement

3.   Adopt emerging technologies to counter AI-enabled crime.

Criminals are using AI to launder illicit funds and perpetrate crimes including fraud. Law enforcement must respond in kind, deploying AI responsibly to accelerate investigations, analyse unstructured intelligence, and integrate multi-modal data sources. The Collaborative Analytics Hub developed by the Fintel Alliance is a great start in that direction. My colleague Mr Craig Robertson will address this.

4.   Prioritise prevention through technology and design audits.

Beyond detecting and disrupting financial crime, we need to focus on prevention. We recommend regular dark pattern audits for large digital platforms and the implementation of easy-exit subscription standards. Partnerships with CSIRO and universities should advance detection technologies and provide specialised training for regulators and law enforcement. **My colleague Dr Nui Surachartkumtonkun will discuss this.**

In closing, the Committee faces a profound challenge: how to equip law enforcement for a future where financial crime is increasingly digital, decentralised, and automated. To tackle this Australia needs a working strategy to fight financial crime. A great example of this can be done can found in the UK's first Economic Crime Plan (2019-2022) in which for the first time the government, law enforcement, supervisory agencies and the private sector jointly developed a set of activities in the UK to reduce money laundering and recover more criminal assets, combat kleptocracy and drive down sanctions evasion, and cut fraud.

If we fail to act decisively as a society, Australia risks becoming a safe haven for technologically enabled criminal networks. But with investment in strategy, skills and collaboration, we can turn this challenge into an opportunity and build a system that is world leading.

Thank you. I look forward to your questions.

Professor Andreas Chai
Director, Academy of Excellence in Financial Crime Investigation and Compliance