GRIFFITH UNIVERSITY

# Submission to the Parliamentary Joint Committee on Law Enforcement's Inquiry into the Capability of Law Enforcement to Respond to Money Laundering and Financial Crime

Griffith Business School
**Professor Andreas Chai**
*Director, Academy of Excellence in Financial Crime Investigation and Compliance*

2 September 2025

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

Dear Sir/Madam,

**Re: Submission to Joint Committee on Law Enforcement's Inquiry into the capability of law enforcement to respond to money laundering and financial crime.**

We appreciate the invitation to make a submission to this consultation exercise. This submission was co-authored by the following researchers and practitioners:

- Professor Andreas Chai, Director of the Academy of Excellence in Financial Crime Investigation and Compliance, Griffith Business School, Griffith University.
- Dr Carys Chan, Senior Lecturer, Griffith Business School, Griffith University.
- Professor Louis De Koker, La Trobe Law School, La Trobe University.
- Dr Gordon Hook, former APG Executive Secretary and Senior Industry Fellow at the Academy of Excellence in Financial Crime Investigation and Compliance, Griffith Business School, Griffith University.
- Craig Robertson Financial Crime Subject Matter Expert (Asia Pacific) Symphony AI and Senior Industry Fellow at the Academy of Excellence in Financial Crime Investigation and Compliance, Griffith Business School, Griffith University.
- Dr Jiraporn (Nui) Surachartkumtonkun, Senior Lecturer, Griffith Business School, Griffith University.

Please do not hesitate to contact the Academy of Excellence in Financial Crime Investigation and Compliance team on [redacted] if you have any questions regarding the following submission.

Yours Sincerely,

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

# Background

Australia is one of the founding members of the Financial Action Task Force (FATF) in 1989, and the Asia/Pacific Group in Money Laundering (APG) in 1997, the regional FATF body for the Indo-Pacific. Membership in these inter-governmental organisations requires Australia to clearly commit on an on-going basis at the highest political level to the full implementation of the FATF 40 Recommendations. These standards have been acknowledged by the UN Security Council since 2005[1] as the international benchmark for an effective legal, regulatory and law enforcement system to combat the threats of money laundering, terrorist financing and proliferation financing of Weapons of Mass Destruction, and of serious financial crime more generally.

The overall objective of the FATF 40 Recommendations is to protect the integrity of the international financial system from the threats posed by money laundering, the financing of terrorism and proliferation financing, thereby strengthening financial sector integrity and contributing to safety and security. Protecting the integrity of the financial system is affected not simply by requiring AML/CTF laws and regulations to be in place but by effective supervisory oversight to ensure that reporting entities comply with their obligations and by imposing sanctions and penalties when they do not. A key component of the FATF Recommendations relate to law enforcement authorities and their powers.

Since Australia joined the FATF it has been the subject of three comprehensive mutual evaluations for compliance with the FATF Recommendations: the first in 1996; the second in 2005; and the most recent in 2015. Australia's next evaluation is scheduled to commence in 2026.

# Objectives of the Inquiry

On 19 June 2024, the Parliamentary Joint Committee on Law Enforcement agreed to inquire into and report on the capability of law enforcement to respond to money laundering and financial crime, including:

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 comparisons with other jurisdictions and the international standards set by the Financial Action Task Force;

c) 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;

d) the effectiveness of collaboration, coordination and information sharing between Commonwealth agencies, including law enforcement, and with authorities in other jurisdictions and the private sector;

[1] S/RES/1617, (2005) 29 July 2005.

e) 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;

f) the operation of unexplained wealth and asset recovery legislation, the Criminal Assets Confiscation Taskforce, and the Confiscated Assets Account; and

g) any related matters.

# Managing the trade-off between intelligence objectives and tranche II implementation

The extension of AML/CTF obligations to tranche II entities are in part intended to increase the flow of financial intelligence to AUSTRAC and law enforcement agencies. There is however a tension between the intelligence objectives of AML/CTF measures and their regulatory objectives to protect AML/CTF-regulated entities against criminal abuse: As customer due diligence measures take effect reporting entities are more protected against criminal abuse and therefore their ability to provide meaningful AML/CTF intelligence declines.

There is however an elevated risk that intelligence flows may be adversely affected while newly regulated entities adopt new risk-based compliance measures. Crime risk assessments are not precise empirical exercises but rather subjective judgment-based conclusions on threats, vulnerabilities and consequences[2]. In some cases, risks may be underestimated while in other cases they may be overestimated. When that happens, regulated institutions may limit or deny services to a range of clients. In banking this has become known as "de-banking" or "de-risking".[3] In practice, denials of service displace criminal money flows. It directs these flows to institutions with weaker control measures and into transactions and channels that are often more difficult to police, for example the cash-based economy, trade-based money laundering, and digital assets. Unless risk-based compliance processes are appropriately supported and monitored they may therefore add new law enforcement challenges.

**RECOMMENDATION 1: Law enforcement agencies should be required and funded (i) to continuously share appropriate data with reporting entities to inform reasonable and data-driven money laundering, terrorist financing and proliferation financing risk assessments; and (ii) to work with industry bodies to identify and help to correct underestimation and overestimation of risks as well as the design of risk control measures that are not commensurate to the assessment risks.**

Tranche II institutions will also have to grapple with the implementation of proliferation financing risk assessment measures. In 2020 the Australian government supported an amendment of the Financial Action Task Force standards that require all countries to undertake national proliferation financing risk assessments and to compel their AML/CTF-regulated institutions to undertake such institutional assessments. AUSTRAC published Australia's first national proliferation financing risk assessment in 2022[4].

[2] De Koker, L., Goldbarsht, D. (2024). FATF's Risk-Based Approach: Has the Pendulum Swung too Far? In: Goldbarsht, D., de Koker, L. (eds) Financial Crime and the Law. Ius Gentium: Comparative Perspectives on Law and Justice, vol 115. Springer, Cham. https://doi.org/10.1007/978-3-031-59543-1_10.

[3] D'Hulster, Morris, Jaffer and De Koker. 2023. The Decline of Correspondent Banking in Pacific Island Countries. World Bank Report. Pacific Islands Forum. https://forumsec.org/sites/default/files/2024-05/CBR%20Report_FINAL.pdf.

[4] AUSTRAC (2022) Proliferation Financing in Australia: National risk assessment. https://www.austrac.gov.au/sites/default/files/2022-12/AUSTRAC_Proliferation_Financing_in_Australia-National_Risk_%20Assessment_Web.pdf.

Proliferation financing risk assessment is more challenging than money laundering and terrorist financing risk assessment as the subject matter is more technical and scientific in nature and requires an appropriate understanding of exports and export control measures as well as appropriate levels of geopolitical knowledge.[5] Depending on how the risk assessment obligations are structured and the extent to which this obligation will be enforced through criminal penalties this obligation may have a significant impact on law enforcement agencies.

**RECOMMENDATION 2: Consider the impact of institutional proliferation financing risk assessment obligations on law enforcement resources.**

## Building a National Training Framework and Research Capacity to Support Law Enforcement Capability

Compared to the US and EU, currently the workforce training landscape for Financial Crime Investigation professionals working across law enforcement and in the financial sector is relatively underdeveloped in Australia. As a result, Australia is at risk of facing critical skill shortages in this area.[6] We encourage the Parliamentary Joint Committee to call on the Federal Government to conduct a skills audit to determine what skills and professional training programs are required by professional investigators located across government agencies, law enforcement and financial institutions that are responsible for actively monitoring and reporting financial crime. These risks should be catalogued and incorporated into the National Skills Taxonomy (run by Jobs and Skills Australia) to help identify and address emerging skills needs, enhance training and education efforts and ultimately help ensure there exists a pipeline of future talent for this critical workforce. Further consideration needs to be given about how to develop a pipeline of talent from universities that law enforcement can draw on to meet their workforce needs in these critical areas. Based on Griffith University's assessment in developing the recently launched Masters 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 a number of different academic disciplines, including criminology, forensic accounting and IT.

These include:

1. Investigative techniques and practical skills required to investigate and report suspicious activity in written form.
2. A basic understanding of the criminological theory of victims and offenders typically involved in financial crimes, as well as the reporting obligation of reporting entities under the new regime.

[5] De Koker, L. (2024). The FATF's Combating of Financing of Proliferation Standards: Private Sector Implementation Challenges. In: Goldbarsht, D., de Koker, L. (eds) Financial Crime and the Law. Ius Gentium: Comparative Perspectives on Law and Justice, vol 115. Springer, Cham. https://doi.org/10.1007/978-3-031-59543-1_6.

[6] Sydney Morning Herald (2021) Absolutely fundamental': Financial crime skills shortage sparks calls for law change, article published July 1 2021, accessed at: https://www.smh.com.au/business/banking-and-finance/absolutely-fundamental-financial-crime-skills-shortage-sparks-calls-for-law-change-20210630-p585ii.html.

3. Accounting skills required in the forensic analysis of financial transactions and financial statements typically used in KYC processes to identify Source of Funds/Source of Wealth (SoF/SoW).
4. Skills to employ data analysis, AI tools and visualisation techniques for detecting suspicious transactions and transaction monitoring.
5. Analytical skills required in conducting risk assessments of customers, and producing, as well as implementing, a risk-based approach from an enterprise perspective. This should include a basic understanding of statistics, and tail risks and using monte carlo simulations for risk assessments.

Universities can play a key role is assisting with developing career pathways into law enforcement from areas such as forensic accounting & and IT.

**RECOMMENDATION 3: The Commonwealth government should conduct skills audits to determine what skills and professional training programs are required by professional investigators located across government agencies, law enforcement and financial institutions that are responsible for actively monitoring and reporting financial crime. These risks should be catalogued and incorporated into the National**

Beyond workforce skills, law enforcement capabilities can also be supported by developing public/private partnerships. The FATF has encouraged the member countries to develop public-private partnerships to grow national capabilities in countering ML and TF threats[7]. In this regard, we encourage the joint Committee to consider how to promote greater data sharing arrangements between regulated entities and universities. Universities can play a crucial role and their research expertise is harnessed to support Australia's law enforcement capabilities. Academic researchers from various disciplines, such as Law, Criminology, Forensic Accounting, and ICT, can generate new knowledge about financial crimes such as money laundering, terrorist financing, and fraud, as well as the compliance challenges that are faced by regulated entities. Increasing the depth and scope of publications on financial crime typologies can help ensure a wide variety of regulated entities have cost effective access to knowledge that can help improve their approaches to monitoring and reporting suspicious behaviour, as well as conducting risk assessments.

A good example of public-private partnerships featuring universities is EuroDaT in Germany which aims to build a European data trustee that enables data sharing, with a focus on financial data, and is being developed in collaboration with the University of Saarland and Goethe University Frankfurt.

Overall, prioritising financial crime as a new national research priority in Australia's Science and Research priorities is essential. Australia's Science and Research Priorities serve to incentivise researchers to focus on areas of strategic national importance.[8] The overall goal of this

**RECOMMENDATION 4: Research into financial crime, in particular money laundering and terrorist financing, be added as a new national priority in Australia's Science and Research Priorities.**

[7] FATF (2022), Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing, FATF, Paris, France.

[8] Australian Government. (2015). Science and Research Priorities. Fact Sheet.

initiative is to help Australia achieve its economic, social, and environmental objectives by supporting research that tackles important national policy issues. Encouraging researchers to focus on financial crime can help to create a more action-oriented and responsive research environment, something sorely needed. Additionally, this would help strengthen Australia's reputation as a leader in the fight against financial crime.

## The Challenge of Emerging Technologies and Promoting Greater Information Sharing Arrangements

**RECOMMENDATION 5: The Australian Government should expedite the implementation of tranche II AML/CTF obligations for designated non-financial businesses and professions (DNFBPs), including lawyers, accountants, and real estate agents. This should be coupled with the establishment of a centralised intelligence-sharing platform that enables real-time information exchange between AUSTRAC, AFP, state police forces, and other relevant agencies, following successful models implemented in the UK and Canada.**

One of the most critical gaps in Australia's current anti-money laundering (AML) framework is the limited information sharing between law enforcement agencies and the exclusion of tranche II entities from suspicious transaction reporting requirements. As highlighted in Bociga et al. (2025)[9], effective money laundering investigations require coordinated cooperation between diverse law enforcement agencies, financial institutions, and other legal entities, yet current mechanisms suffer from fragmented approaches and lack of standardised procedures. Research by Bondarenko et al. (2024)[10] emphasises that methodological principles of cooperation between law enforcement agencies in combating money laundering are currently set out in normative sources quite fragmentarily, without defining specific boundaries, scope and degree of cooperation. The absence of suspicious transaction reports from lawyers, accountants, real estate agents, and other designated non-financial businesses and professions creates significant intelligence blind spots that criminals can exploit. Research demonstrates that countries like New Zealand, Canada, and the UK, which have successfully integrated these sectors into their AML frameworks, provide law enforcement with substantially more comprehensive intelligence to identify, freeze, and seize criminal proceeds.[11]

### *Collaboration*

For the new AML/CTF regime to work effectively, it is important to create an institutional environment that is conducive to enabling research and collaboration that can be used by reporting entities to identify and mitigate the risks of financial crime. The Committee should consider what provisions can be made to encourage law enforcement industry and regulators

[9] Bociga, D., Lord, N., & Bellotti, E. (2025). Dare to share: information and intelligence sharing within the UK's anti-money laundering regime. *Policing and Society*, 35(6), 812-831. https://doi.org/10.1080/10439463.2024.2428735

[10] Bondarenko, O., Utkina, M., Reznik, O., & Dumchikov, M. (2024). Mechanisms for interaction of law enforcement agencies in the field of countering money laundering. Journal of Money Laundering Control, 27(1), 34-50. https://doi.org/10.1108/JMLC-01-2023-0006

[11] FATF. (2018). *Anti-money laundering and counter-terrorist financing measures: United Kingdom Mutual Evaluation Report*. FATF. https://www.fatf-gafi.org/content/dam/fatf-gafi/mer/MER-United-Kingdom-2018.pdf.coredownload.inline.pdf

to work together to share information and collaborate with industry, both to investigate criminal threats and develop law enforcement AI capability.

As recently noted by the FATF:

> *"Collaboration and information sharing helps financial institutions to build a clearer picture of criminal networks and suspicious transactions, and better understand, assess, and mitigate their money laundering (ML), terrorist financing (TF) and proliferation financing (PF) risks. It can also provide authorities with better quality intelligence to investigate and prosecute these crimes and ultimately help prevent crime from reaching our streets."*[12]

Law enforcement agency adoption of emerging technology including artificial intelligence (AI), will require a partnership across industry, law enforcement and regulators. With criminal actors leveraging the latest in technology to commit crimes, law enforcement agencies will require capability to counter criminal threats and conduct complex investigations. AI offers law enforcement a combination of individual detection models, augment investigation processes and the opportunity to radically improve the efficiency and robustness of investigations.

### *Enhancing Investigations using LLMs and AI*

The investigation of financial crime threats is a time-consuming process, which relies on many human resources. The key task in this process is for humans to understand the volume of financial intelligence and apply their judgement about criminal risks. Currently, much of the time is spent performing pre-determined tasks, including:

- Understanding current and previously identified risks (review of unstructured intelligence reporting),
- Background research (searching for relating intelligence and connections), and
- Behavioural analysis (accessing and reviewing transactional data from financial services, communications and social media sources).

Large language models (LLM), with the correct guard rails and protocols in place, are well suited to accelerating and supporting human activities in these areas. Key technologies in this area are *chain of thought prompting* and *retrieval augmented generation*, that structure the responses of the LLM and ground them in trusted data sources and statistical models, guiding law enforcement investigators to focus on key risks.

Previously, it was very difficult to combine unstructured intelligence reporting with structured models seeking to highlight risks. With the availability of deep learning models able to process, structure, and tag unstructured data in all formats, multi-modal models are beginning to emerge and, with the addition of new industries to the AML/CTF framework, will assist law enforcement in handling new sources of financial intelligence. In law enforcement investigations, this technology can make an impact in areas such as:

- Analysing customer and payment records,

[12] FATF (2022), Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing, FATF, Paris, France.

- Verifying risk attributes about known criminals, and
- Accurate leveraging of all source intelligence (including in multiple formats e.g. video, data).

Using AI to rationalise and incorporate these sources into existing risk evaluation processes can further improve the effectiveness and efficiency of law enforcement financial crime investigations. At the same time, it is important to acknowledge that AI needs to be implemented in a responsible and ethical manner. Adopting an AI-driven approach to detect and investigate financial crime, must have design principles that are:

- Relevant to particular risk criminal activity profiles (e.g. laundering the proceeds of trafficking drugs),
- Robust to "blind spots" in an organisation's historic data and intelligence holdings, and
- Explainable and interpretable to a variety of stakeholders including investigators, prosecutors and regulatory bodies.

**RECOMMENDATION 6: Law enforcement should adopt emerging technology in collaboration with industry, and to enhance investigations and counter the use of AI and similar technology advances to commit crime and launder proceeds.**

To maximise these capabilities and ensure AI is implemented responsibly, law enforcement agencies need to incorporate AI skills into their workforce plans and ensure there is adequate budget in professional development programs that can enable law enforcement agencies to get their workforce adequately trained via courses or micro-credentials offered by tertiary institutions, such as Griffith University.

**RECOMMENDATION 7: Law enforcement agencies need to incorporate AI skills into their workforce plans and ensure there is adequate budget in professional development programs that can enable law enforcement agencies to get their workforce adequately trained.**

Many of Australia's state law enforcement agencies are dedicating considerable resources to public information campaigns to grow public awareness of scams and cybersecurity threats. Scams are a particular type of financial crime that not only lead to direct financial losses, they also have a detrimental impact on mental health, relationships and job prospects. A recent study of scams identified more than 20 varieties of online scams that have a major impact on well-being, with 500,000 people estimated as victims of modern slavery and numerous suicides taking place as a result of specific types of scams like sextortion[13]. According to Interpol Secretary General, Juergen Stock "we are facing an epidemic in the growth of financial

[13] GCFFC Asia Chapter (2024) Financial Scams Report: An Assessment of Scams in East Asia https://www.gcffc.org/wp-content/uploads/2024/06/GCFFC-Scams-Report-6June2024Pbd-3.pdf.

fraud, leading to individuals, often vulnerable people, & companies being defrauded on a massive and global scale"[14].

There is a growing and largely unmet need to promote public education and develop tech solutions to protect the public. Most people remain unaware of how easily deepfakes can be created or how sophisticated phishing attacks have become, leaving them more vulnerable to falling prey to these high-tech scams. While some measures, such as Scamwatch, are helping to disrupt scams and inform the public who are actively searching for information online, there is still a need to heighten levels of awareness among the vulnerable before they are targeted by scammers, equipping the public with new tools to help them discern, detect and report scams.

It is vital to develop new tech solutions that can reach an audience and assist people who may be under attack from scammers in real time. In this regard AI and LLMs can also be of assistance:

- LLMs can be used to build chatbots for the detection of online scams that could be used by members of the public to receive customised real time advice about what potential warning signs to look for in their particular situation. Chatbots are conversational programs designed to show humanlike behaviour by mimicking text- or voice-based conversation. Evidence suggests that people are more likely to feel more anonymous when interacting with chatbots, which can assist in helping victims of scams in feeling comfortable in discussing scams[15].
- AI technology can be used to develop deepfake detection tools that enable users to conduct due diligence on suspicious videos and audio messages.

**RECOMMENDATION 8: Law enforcement adopt AI to support prevention and public awareness and education campaigns, including chatbots, community scam forums and online scam content.**

[14] GCFFC Asia Chapter (2024) Financial Scams Report: An Assessment of Scams in East Asia https://www.gcffc.org/wp-content/uploads/2024/06/GCFFC-Scams-Report-6June2024Pbd-3.pdf.

[15] Croes, E. A., & Antheunis, M. L. (2021). 36 questions to loving a chatbot: are people willing to self-disclose to a chatbot? In Chatbot Research and Design: 4th International Workshop, CONVERSATIONS 2020, Virtual Event, November 23–24, 2020, Revised Selected Papers 4 (pp. 81-95). Springer International Publishing.

# Dark Patterns and Law Enforcement Capability

Dark patterns—manipulative online interface designs that exploit cognitive biases—are increasingly recognised as both an unfair trading practice and, at their extreme, an enabler of scams, fraud, and money laundering. Research shows 83% of Australians report negative impacts from manipulative designs, with younger consumers especially vulnerable. [16] Internationally, regulators are moving to address these practices: the EU's Digital Services Act prohibits manipulative interfaces, while the UK's Digital Markets, Competition and Consumers Act 2024 empowers the Competition and Markets Authority to act directly against harmful "online choice architecture." In the United States, "click-to-cancel" subscription standards and state-level rules voiding consent obtained via dark patterns are being introduced.[17] [18] At the same time, technical innovations in Australia and overseas provide tools for monitoring. For example, recent work has demonstrated AI-driven detection systems that combine webpage structure, visual cues, and text analysis[19], as well as dynamic testing tools such as AppRay, developed by CSIRO with university partners, which detect manipulative designs in mobile apps in real time.[20] Together these developments highlight the need for both regulatory clarity and investment in monitoring capabilities.

**RECOMMENDATION 9: The Australian Government should empower the ACCC, in collaboration with AUSTRAC and the OAIC, to establish a dedicated Dark Pattern Monitoring and Enforcement Unit. This unit should deploy AI-enabled detection systems and mandate regular "dark pattern audits" for large digital platforms. It should also oversee implementation of easy-exit subscription standards (e.g., click-to-cancel) and ensure that consent gained through manipulative design is legally voidable. Partnerships with CSIRO and universities should be developed to advance detection technologies and provide specialised training for regulators and law enforcement.**

[16] Consumer Policy Research Centre (CPRC). (2025). Made to manipulate: Manipulative online design in Australia. Melbourne: CPRC. https://cprc.org.au/report/made-to-manipulate-report/
[17] OECD. (2022). Dark commercial patterns. OECD Digital Economy Papers, No. 321. Paris: OECD Publishing. Dark commercial patterns | OECD
[18] Australian Treasury. (2024). Unfair trading practices: Options paper. Canberra: Commonwealth of Australia. https://treasury.gov.au/consultation/c2024-602157
[19] Bajaj, A., Uppal, K., Razdan, R., Tuteja, Y., Bhardwaj, A., & Abraham, A. (2025). A Comprehensive Analysis for Dark Pattern Detection Using Structural, Visual and Textual Information. *International Journal of Computer Information Systems and Industrial Management Applications*, *17*, 12-12.
[20] Xia, L., Wu, C., Li, Z., Liu, J., & Zhang, Y. (2024). AppRay: Dynamic detection of dark patterns in mobile applications. arXiv preprint arXiv:2411.18084. https://arxiv.org/abs/2411.18084

## Evidence-Based Policing and Effectiveness Measurement

A fundamental challenge facing Australian law enforcement is the lack of empirical evidence demonstrating which AML measures actually work in reducing criminal activity. Hock et al. (2023)[21] conducted a comprehensive literature review of over 1,000 sources on money laundering policing and found that despite the vast expansion of AML scholarship, "not a single study on money laundering establishes a correlation between a money laundering prevention program and money laundering risk factors at a single point in time." This absence of evidence-based evaluation severely hampers law enforcement's ability to allocate resources effectively and develop targeted strategies. Without systematic data collection and analysis of outcomes, such as the actual amount of money laundered versus prevented, law enforcement agencies cannot demonstrate the effectiveness of their interventions or justify resource allocation decisions to government and the public.

**RECOMMENDATION 10: Law enforcement agencies should be required and funded (i) to continuously share appropriate data with reporting entities to inform reasonable and data driven money laundering, terrorist financing and proliferation financing risk assessments; and (ii) to work with industry bodies to identify and help to correct underestimation and overestimation of risks as well as the design of risk control measures that are not commensurate to the assessment risks.**

## Technology Adoption and Workforce Development

The rapid evolution of financial crime methods, particularly through emerging technologies and artificial intelligence (AI), requires law enforcement to develop sophisticated technological capabilities and appropriately skilled workforces. However, Australia faces critical skill shortages in financial crime investigation, with the workforce training landscape significantly underdeveloped compared to the US and EU[22]. Law enforcement agencies need substantial investment in AI-powered investigation tools, large language models for processing unstructured intelligence data, and advanced analytics for transaction monitoring. Furthermore, as criminals increasingly leverage AI for sophisticated fraud and money laundering schemes, law enforcement must develop parallel capabilities to detect deepfakes, analyse complex digital transactions, and conduct investigations across multiple digital platforms. The growing threat of financial scams, which according to recent research affects over 500,000 people as victims of modern slavery with numerous suicides resulting from specific types like sextortion,[23] demonstrates the urgent need for enhanced technological capabilities. This technological arms race requires sustained investment in both technology infrastructure and workforce development, including partnerships with universities to create career pathways from fields like forensic accounting, criminology, and information technology into law enforcement roles. As noted by FATF (2022)[24], collaboration and information sharing

[21] Hock, B., Button, M., Shepherd, D., & Gilmour, P. M. (2023). What works in policing money laundering? Journal of Money Laundering Control, 27(1), 5-13. https://doi.org/10.1108/JMLC-07-2023-0109
[22] Grieve, C. (2021, July 1). 'Absolutely fundamental': Financial crime skills shortage sparks calls for law change. Sydney Morning Herald. https://www.smh.com.au/business/banking-and-finance/absolutely-fundamental-financial-crime-skills-shortage-sparks-calls-for-law-change-20210630-p585ii.html
[23] GCFFC Asia Chapter. (2024). *Financial Scams Report: An Assessment of Scams in East Asia*. https://www.gcffc.org/wp-content/uploads/2024/06/GCFFC-Scams-Report-6June2024Pbd-3.pdf
[24] FATF. (2022). Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing. FATF. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf

between financial institutions and law enforcement helps build clearer pictures of criminal networks and better quality intelligence for investigations.

**RECOMMENDATION 11: The Australian Government should establish a National Financial Crime Technology Hub within the AFP or AUSTRAC, with dedicated funding for AI-powered investigation tools, advanced analytics capabilities, and workforce development programs. This should include partnerships with universities to create specialised degree programs in financial crime investigation and mandatory continuing professional development for law enforcement officers working in financial crime units. Additionally, implement a national certification program for financial crime investigators to ensure consistent skill standards across all jurisdictions.**

GRIFFITH UNIVERSITY
QUEENSLAND AUSTRALIA

CRICOS: 00233E | TEQSA: PRV12076