FINANCIAL INTEGRITY HUB INSIGHTS

March Issue 2025

FINANCIAL INTEGRITY HUB

MACQUARIE University
SYDNEY·AUSTRALIA

LEADERSHIP

Patron
Honourable Patricia Bergin AO SC

Director
Associate Professor Doron Goldbarsht

Associate Director
Isabelle Nicolas

Advisory Board
Armina Antoniou
Stuart Clark AM
Professor Louis De Koker
Paul Jevtovic APM OAM
Professor Elizabeth Sheedy
Michael Tooma

Reference Group
Sue Bradford
Jeremy Moller
Tony Prior

Research Fellows
Dr Daley Birkett
Dr Derwent Coshott
Dr Jamie Ferrill
Dr Hannah Harris

Researchers
Giang Nguyen
Ben Scott

Interns
Soha Khan
Benjamin Mensah
Jade Reuveny
Dana Schmidt

Citing reference: Financial Integrity Hub 'FIH Insights' (2025) 1(1) FIH, Sydney
<https://www.mq.edu.au/research/research-centres-groups-and-facilities/groups/financial-integrity-hub/engagement>.

ABOUT US

The Financial Integrity Hub (FIH) is a leading research center dedicated to financial crime prevention and mitigation. Our mission is to foster collaborative partnerships that strengthen research, policy, and practice, ensuring a robust and resilient financial system.

At FIH, we actively engage with academia, government, and industry to develop innovative, evidence-based solutions that address the complexities of financial crime. Our research is designed not only to advance academic understanding but also to influence regulatory frameworks, enhance enforcement strategies, and shape industry best practices.

By bridging the gap between theory and real-world application, we contribute meaningfully to financial integrity, compliance effectiveness, and policy reform. Through thought leadership and collaborative dialogue, we strive to create a more transparent, accountable, and secure financial landscape.

We extend our appreciation to our authors and contributors, whose expert insights and analyses allow us to deliver timely updates, valuable perspectives, and thought-provoking content to our readers.

Together, we can drive progress in the fight against financial crime and work towards a stronger, more resilient financial system.

CONTACT US
Financial Integrity Hub
Michael Kirby Building Macquarie University
NSW 2109, Australia
E: fih@mq.edu.au T: +61 (2) 9850 7074

Follow us here:

We thank our partner, WhiteLight AML, for their support. Since 2019, WhiteLight AML has been Australia's trusted partner in navigating the complexities of AML and CTF. Specialising in risk assessments and tailored AML/CTF programs, they ensure comprehensive compliance. With fully outsourced AML/CTF operations, they take the burden off your shoulders, allowing you to focus on what you do best!

TABLE OF CONTENTS

PERSPECTIVES ON PRIVATE-TO-PRIVATE INFORMATION SHARING AT THE SOUTH AFRICAN FINANCIAL CRIME SYMPOSIUM

Image: Taken at the South African Financial Crime Symposium.

Professional money laundering activities often manifest as intricate operations spanning multiple accounts and institutions, exploiting the fragmented nature of traditional financial crime detection systems. Historically, financial institutions have analysed their data in isolation, focusing solely on internal transactions, which impedes their capacity to detect broader, interconnected criminal networks. Criminal organisations capitalise on this fragmentation, conducting transactions across various entities, thereby complicating authorities' ability to identify suspicious activity effectively. However, the advent of Private-to-Private (P2P) information sharing presents a promising solution to this challenge, offering significant advantages in detecting, preventing, and disrupting financial crime.

In early March, the South African Financial Crime Symposium - organised by the Financial Sector Conduct Authority and the Unit for Corruption and Integrity Studies at the North-West University Business School (with Albert van Zyl leading the charge), brought together a room full of sharp minds to tackle the big questions about keeping financial systems safe. The interactive panel discussions at this year's symposium explored a wide array of topics, including fraud in deceased estates, the response to kidnapping and extortion, security risk assessments for financial investigators and law enforcement, and the use of artificial intelligence in combating money laundering and terrorist financing. It became evident that economically motivated criminals operate as sophisticated enterprises, embracing technology, utilising professional enablers, and transgressing national boundaries. Particularly concerning is their evolving modus operandi, which not only poses significant risks to the users of banking applications but also threatens the safety of those who challenge their criminal enterprises.

The symposium highlighted a key theme: collaboration. Public and private sectors need to join forces and share information if we're going to stay ahead of the game. South Africa's journey as a grey-listed country by the Financial Action Task Force (FATF) has shown us that lessons can be learned, but we need to act fast.

Looking at the bigger picture, public-private partnerships (PPPs) for information-sharing have come a long way since 2015. Here are some milestones that show how these collaborations are transforming the fight against financial crime:

- The UK piloted the Joint Money Laundering Intelligence Task Force (JMLIT) in 2015.
- Canada followed in 2016 with its first partnership initiative under the "Project".
- Australia launched the Fintel Alliance in March 2017.
- Other notable initiatives include the Singapore Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership (ACIP) in April 2017, the Netherlands Terrorist Financing Taskforce (NL-TFTF) in July 2017, the New Zealand Financial Crime Prevention Network (NZ-FCPN) in December 2017, and South Africa in December 2019 with the South African Anti-Money Laundering Integrated Task Force (SAMLIT).

These partnerships reflect a global shift toward collaborative approaches to financial crime detection and prevention. As articulated by Dr Doron Goldbarsht, the "next frontier" in financial crime intelligence sharing is Private-to-Private (P2P) information sharing, which was addressed in a pivotal session of the symposium.

Private-to-Private Information Sharing

The symposium featured a panel of thought leaders from the banking sector, financial regulatory bodies, constitutional and privacy law, and international experts, who introduced the need for, enabling mechanisms of, and practical steps toward enhancing private-private information sharing. Dr Goldbarsht emphasised that, given the growing sophistication of financial crime, enhanced cooperation - especially through information sharing - is critical to strengthening detection and prevention efforts and maintaining global financial integrity. He pointed to the global shift toward collaborative approaches to financial crime detection and prevention, noting that the evolution of public-private information sharing, from a novel concept to a foundational element in combating financial crime within liberal democracies, signals the urgency of advancing P2P information sharing as the next frontier.

The key benefits of P2P information sharing highlighted during the panel discussions include enhanced detection and disruption of financial crime, greater operational efficiency, real-time sharing of information, and a positive impact on de-risking. While the panel discussed the interpretation of private information, the potential concerns of regulated entities, and the possibility of leaving privacy breaches to judicial determination, it was suggested that adopting a P2P model is not a straightforward task and must be approached with careful consideration.

Crucial considerations for financial institutions and regulators in developing effective P2P models include legal and regulatory concerns, banking secrecy, and the operational challenges inherent in creating secure and efficient information-sharing systems. Further deliberation is needed on several practical matters: what information should be shared (e.g., KYC data, Suspicious Activity Reports), who should bear the cost of the platform, who should manage the platform, whether participation should be voluntary or mandatory, and the potential risks and threats associated with these decisions. Moreover, the initiative calls for the involvement of not just the banking sector but also other reporting entities, broadening the scope and impact of the information-sharing framework.

Ultimately, P2P information sharing could be the next big thing in global financial crime detection. With a little more cooperation and innovation, we might just be able to turn the tables on the criminals who have been slipping through the cracks for far too long. The symposium concluded with a series of actionable steps to advance the development and implementation of a P2P model for South Africa. The importance of academia in this process was acknowledged, and the possibility of future collaboration with the Financial Integrity Hub was enthusiastically welcomed.

THE FUTURE OF INFORMATION SHARING - THE NEW TIPPING-OFF OFFENCE

Neil Jeans

The new tipping-off offence, which becomes effective on 31 March 2025, marks a critical evolution in Australia's approach to combating financial crime. It represents a significant shift in focus, addresses existing limitations, and facilitates better information sharing within and among reporting entities and with third parties.

The primary change involves a redefinition of what constitutes "tipping-off". Previously, under Section 123 of the Anti Money Laundering Counter Terrorism Financing Act 2006 Cth ('AML/CTF Act'), reporting entities were prohibited from disclosing to customers or third parties that a suspicious matter report (SMR) had been or would be filed with AUSTRAC.

The rigid nature of the old tipping-off regime often led to operational challenges for businesses, particularly those operating within complex corporate structures or across multiple jurisdictions. The old tipping-off offence inadvertently stifled legitimate information sharing, thereby hampering effective risk management and compliance efforts.

The new tipping-off offence reframes this prohibition to focus on preventing disclosures that could reasonably prejudice an investigation. This shift allows for more nuanced and context-specific applications of the law, reducing the risk of inadvertently hindering legitimate business operations while maintaining the integrity of AML/CTF efforts. The offence is re-focused on the harms that could flow from disclosing information rather than the mere disclosure of information itself.

The evolving nature of financial crime seeks to exploit any gaps in the regulatory regime. The updated tipping-off provisions aim to close one of these gaps by allowing for more effective internal communication and coordination among reporting entities, thereby enhancing their ability to detect and prevent illicit activities. Who can be guilty of a tipping-off offence has also been clarified, limiting it to only a reporting entity, an officer, employee or agent of a reporting entity, or a person required under a notice to give information or produce documents concerning a report, or to assist the AUSTRAC CEO perform its functions.

The changes to the tipping-off offence are expected to profoundly impact information sharing within and between reporting entities. By focusing on disclosures that could prejudice investigations, the new tipping-off regime will support greater communication about suspicious activities without the fear of breaching the law.

This is particularly important where practical AML/CTF compliance relies on seamless information flow and effective ML/TF risk management, necessitates exchanging information within corporate groups, with third parties such as consultants and contractors, and other reporting entities. Going forward, AML/CTF policies must include appropriate measures to reduce the risk of tipping off by preventing the disclosure of information in a way that could lead to it reaching the subject of an SMR or their associate.

These measures could include restricting who can access the information to those with a genuine need to know, ensuring those who have access to the information have received training on how to reduce the risk of tipping off when interacting with customers, maintaining appropriate information security practices, and attaching conditions to the further use of information provided to third parties to ensure that the information is only disclosed to appropriate people and does not get back to the subject.

If information is being shared overseas, consideration should also be given to the legal obligations that apply to entities in foreign countries, to ensure compliance with the Australian AML/CTF Act and other legal obligations, such as privacy.

The tipping off offence changes follow on the heels of new information sharing powers designed to strengthen AUSTRAC's ability to combat financial crime, which went live on 7 January 2025. Key among these is Section 49B, which allows the AUSTRAC CEO to issue notices compelling individuals or entities to provide information or documents that may assist in AML/CTF efforts. This power is complemented by Section 49C, which authorises voluntary information sharing with AUSTRAC, providing legal protection for those who choose to cooperate. Additionally, Section 172A has introduced compulsory examinations, enabling AUSTRAC to compel individuals to attend examinations and provide evidence or documents relevant to AML/CTF investigations. These enhanced powers are expected to significantly bolster AUSTRAC's investigative capabilities, supporting more robust enforcement of AML/CTF laws.

Redefining the tipping-off offence seeks to improve business compliance and risk management and further aligns Australia's AML/CTF regime with international standards, including those within the Financial Action Task Force (FATF) Recommendations.

Neil Jeans, Risk Consulting Partner at Grant Thornton

TIPPING OFF REFORMS: A VALUABLE ADDITION IN THE FIGHT AGAINST FINANCIAL CRIME

Paddy Oliver

Much has been written about the *AML/CTF Amendment Act*, 2024. One of the major and most requested reforms is in the area of information sharing between reporting entities, commonly known as "tipping off" under the AML/CTF Act, Section 123. In fact, such is the importance of the tipping-off reform that industry successfully lobbied the government to bring forward its introduction by a year from 31 March 2026 to 31 March 2025.

What are the reforms, and why are they so important?

The pre-31 March 2025 Section 123 tipping-off offence had several major drawbacks, which resulted in reporting entities, and people in those entities, being unable to share relevant information about higher-risk customers for fear of criminal prosecution.

Firstly, it was based upon the prohibition of non-disclosure by a reporting entity of a suspicious matter report or, importantly, any information from which it could be reasonably inferred that the reporting entity has given, or is required to give, that report. Therefore, under the wide ambit of the second limb of the offence - reasonable inference - information about a high-risk customer of one reporting entity could not be shared with another reporting entity unless in a designated business group or corporate group.

Secondly, to try to alleviate the strictness of the tipping-off offence, the exceptions to Section 123 had to be amended on a relatively frequent basis. Even with the ever-expanding exemptions, there was still a fear in the regulated population of breaching the tipping-off offence. Another outcome was the numerous AML/CTF Act modification applications to AUSTRAC by reporting entities to form designated business groups to allow those reporting entities falling outside the narrow definition of "designated business group" or "corporate group" to avail of exceptions to the tipping-off offence.

The consequence of the scope of Section 123 is a bias towards higher-risk, potentially criminal, customers who understood that information could not be shared between reporting entities. These customers avoided being subject to enhanced due diligence or more serious sanctions, hardly a policy outcome the AML/CTF Act intended.

The new tipping-off offence centres on preventing the disclosure of a suspicious matter report under section 41 or information relating to a notice issued under sections 49 or 49B where it would reasonably prejudice an investigation into an offence against the Commonwealth, a State or Territory, or the Proceeds of Crime Act.

The new definition and exceptions will allow information to be disclosed between reporting entities when “the disclosure is made for the purpose of detecting, deterring, or disrupting money laundering, the financing of terrorism, proliferation financing, or other serious crimes.” Reporting entities will now be able to share information about higher-risk customers, which previously, under the pre-31 March 2025 section, would have been a criminal offence.

Risks do arise from the new offence. Reporting entities must design and implement robust controls to ensure that information that would prejudice an investigation is not disclosed deliberately or inadvertently. These controls must be internal to the reporting entity and across all the relationships that a reporting entity might have for information sharing, including the giving and receiving of information to and from third parties, for example, outsourced transaction monitoring service providers. These controls must be well-designed and subject to frequent testing and quality assurance.

The fact that reporting entities, particularly the banks, lobbied for the new section to be implemented a year earlier than originally intended shows that they want tools to fight financial crime. The post-31 March 2025 Section 123 goes a long way toward providing those tools.

Paddy Oliver, Director & Principal, AML Experts Consulting & Legal

TAKING A STEP BACK: A SYSTEM-LEVEL ANALYSIS OF AUSTRALIA'S AML/CTF REFORMS, THEIR GAPS, AND CONSEQUENCES

Michael Brand

The recent amendments to the AML/CTF Act address many existing pressures: standards have been changed to meet FATF recommendations, “tranche 2” reporting entities have been added to alleviate public pressure for more effective financial supervision, and exceptions have been added to the "tipping off" provisions in response to the banks' outcry for more private-to-private information sharing. But will these changes be effective?

The amendments to the “tipping off” provisions allow financial institutions to share suspicions when disclosure is made to another reporting entity for the purpose of detecting, deterring, or disrupting ML/TF/PF. However, the disclosing institution bears an evidential burden of proof that those conditions were met. Arguably, banks under this system are disincentivised from sharing information, both because the burden of proof in the new legislation exposes them to regulatory risk, and because revealing client information disadvantages banks commercially.

Financial crime is an activity that spans many people and organisations. True financial crime typologies are patterns of financial behaviour that often cross multiple accounts at multiple institutions. And yet, the provisions of the *AML/CTF Act*, both before the amendments and after, have been boxing financial institutions into running AML/CTF programs that consider each account in isolation. Explicitly, both the financial institutions and AUSTRAC are blinded from seeing the very patterns that they are meant to find. The new provisions change the map by allowing reporting entities to report suspicions to other reporting entities, but these would be suspicions that already under the previous system would have been reportable to AUSTRAC. They therefore do not bring new evidence to the FIU. An unintended consequence, however, is that networks of institutions may coordinate risk information in order to jointly debank risky customers. The original legislation expressly forbade such collusion, which gives these networks a commercial advantage against competitors. In terms of effective financial supervision, too, such coordination may be detrimental: if the big four banks displace financial crime to smaller competitors with less mature AML/CTF programs, this will actively push crime to where it is harder to obstruct.

As for benefits, the ultimate result of the new provisions is likely to be confined to the streamlining of operations like the Fintel Alliance. They will allow, for example, AFP-driven operations to proceed faster, with all relevant parties “in the room”. They will not, however, solve the problem that such operations are centred on the verification of pre-existing suspicions, rather than the finding of hitherto unknown crime and criminals, and they will not change the basic equation that increased reporting to AUSTRAC (to spread a wider net on financial crime) is always at the expense of individual privacy, a topic where Australia's laws have up until now been exceptional on the world stage (but now, with “tranche 2”, permit solicitation of information from, e.g., lawyers, conveyancers and accountants).

Back in 2019, AUSTRAC commissioned me to come up with a solution that changes this equation, where added financial surveillance does not automatically equate to reduction in privacy. This solution, now named “FinTracer” and released by AUSTRAC in open source, is a system that uses novel Privacy Enhancing Technologies (PETs) in order to allow an FIU to query the entire financial system in one go, looking for the behavioural criminal typologies that have so far been hidden from it, but without any impact on the privacy of uninvolved individuals, without banks having to report any new information, and without any breach of the stricter tipping off provisions that were then current. It is a system with efficacy comparable with analysing all data in one bucket, as is done, for example, in the Netherlands (where five leading banks combine their transaction data to allow its joint analysis), but without all the drawbacks to privacy and information security.

The BIS Innovation Hub's first phase of Project Aurora concluded regarding such methods that “PET-enabled Collaborative Analysis and Learning together with machine learning-based network analysis appears to reduce the number of false positives by up to 80% compared with the siloed rule-based method”. The alternative of better financial supervision with simultaneously better privacy therefore exists. The question is only when we, the public, will begin demanding it of our legislators.

Professor Michael Brand, Director, Otzma Analytics; Adjunct Professor, RMIT University

INTELLIGENCE SHARING AND REFORMS TO THE TIPPING-OFF PROVISIONS

Ben Scott

The Australian government is responsible for enforcing the laws that prohibit money laundering and other serious financial crimes. Intelligence about these crimes is spread across a number of industries, including the financial system. The government needs help to detect it, so financial system actors and other reporting entities have a responsibility to report their suspicions about financial crime to Australia's financial crime intelligence unit and regulator, AUSTRAC. However, this intelligence is extremely sensitive. The government cannot run the risk of accidental disclosure to a criminal group or the tarnishing of an innocent person's reputation based on a mere suspicion. That is the rationale behind tipping-off laws.

Tipping-off is when a reporting entity discloses information relating to a reported suspicion to someone who is not authorised to receive that information. This is an offence. In Australia, amendments to the tipping-off provisions were part of the recent reforms to the *Anti-Money Laundering and Counter-Terrorism Financing Act*, which come into effect in 2025-26.

What was the purpose of these reforms and how will the new tipping-off provisions affect the work of law enforcement agencies, reporting entities and AUSTRAC? The pre-reform tipping-off provisions are broad in scope, and the penalties hefty. Breaching them is a criminal offence, and can result in a penalty of up to two years' imprisonment. This tends to concentrate the minds of lawyers and compliance professionals and create a strong incentive to avoid tipping-off, as it should. However, the breadth of the current provisions has created some unintended consequences.

As it stands, section 123 creates a broad prohibition on disclosing information about a Suspicious Matter Report (SMR) to anyone other than AUSTRAC. That includes anything that could lead a person to draw an inference that an SMR has been or will be reported. There are various exceptions, but they are narrow in scope. Section 123 could be breached, for example, by a reporting entity sharing information about a customer's criminal activity with the police officer investigating that crime. The combination of strict liability with the 'reasonable inference' provision creates a cloud of anxiety that hovers over any conversation between two or more well-meaning people trying to have a productive discussion about a financial crime matter in Australia.

The consequences that flow from the tipping-off provisions have become more restrictive over time. Public-private partnerships like the Fintel Alliance and the UK JMLIT were established in recognition that excellent intelligence outcomes could flow from allowing reporting entities to collaborate directly with the government FIU. This can be facilitated in various ways without breaching tipping-off laws. However, these methods are generally not operationally efficient, and the groundwork of determining whether a proposed collaboration strayed into tipping-off territory is always time-consuming. In this way, provisions designed to stop the deliberate or negligent disclosure of criminal intelligence became an impediment to intelligence practitioners and investigators doing their jobs.

Change was needed, and to their credit, Australian lawmakers have taken a pragmatic approach. The new tipping-off provisions have a sharper focus on the harm they are intended to address. They will refer to the disclosure of information that would or could reasonably be expected to prejudice an investigation. There is also an information sharing exception. Under this exception, the government can make regulations governing information-sharing arrangements. If reporting entities share information as set out in these regulations, for the purpose of detecting, deterring or disrupting financial crime, no breach occurs.

The scope of the new tipping-off provisions remains wide. Differing interpretations of what could reasonably be expected to prejudice an investigation may still limit reporting entities' appetite to collaborate. More effort is needed to provide a reliable framework for information-sharing partnerships based on clear guidance. However, the new provisions provide a better foundation for information-sharing and intelligence collaboration. This is fortunate as the velocity of scams, fraud and other criminal activity requires rapid, effective responses. Some of these must be coordinated by government. There is also a place for peer-to-peer collaboration across Australian businesses within defined guidelines. The next step is to consider the design of regulations to support the information-sharing and intelligence collaboration arrangements Australia needs.

Ben Scott, Head of Data and Technology at the Australian Financial Crime Exchange and Financial Integrity Hub Researcher

INFORMATION SHARING AND AML/CTF - NEW DEVELOPMENTS IN EU LAW

Maxime Lassalle

Within the European Union and beyond, the anti-money laundering (AML) and counter-terrorist financing (CTF) prevention system has been subject to scrutiny, particularly regarding its effectiveness. For instance, in 2017, Europol highlighted the imbalance between the number of reports submitted by obliged entities and the operational usefulness of those reports. In response, the idea of developing public-private partnerships gradually gained traction in the EU, inspired in part by foreign examples such as the Joint Money Laundering Intelligence Taskforce (JMLIT) in the United Kingdom. The Europol Financial Intelligence Public-Private Partnership (EFIPPP) was created in 2017 and some Member States have established their own models. Yet they all had developed in the absence of a European legal framework for information sharing

In 2024, the European legislator adopted the sixth AML package, which significantly transforms the EU's AML/CTF prevention system. This reform introduces various mechanisms designed to facilitate the circulation of financial intelligence, both between the public and private sectors and among obliged entities themselves. This latest reform of the AML/CTF legislation—the third since 2015—reflects a continuous quest for effectiveness in combating money laundering and terrorist financing. The EU's recognition of the need to enhance financial intelligence sharing is primarily reflected in two key ways.

First, Regulation 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing acknowledges in Article 75 the possibility for obliged entities, on a voluntary basis, to engage in information-sharing partnerships. This provision has undoubtedly attracted the most attention. It is subject to numerous conditions, including a requirement for obliged entities to notify national regulators of their intent to participate in such partnerships.

Notably—and somewhat surprisingly—these regulators must verify themselves the partnership's compliance with data protection laws. It should also be noted that the regulation formally limits the data that can be exchanged and sets out several procedural conditions to regulate the creation and use of information-sharing partnerships. For example, it requires a data protection impact assessment, restricts the transfer of data received within the framework of such partnerships, and asks obligated entities to define internal policies aimed at streamlining data processing related to these partnerships. While Article 75 primarily addresses private-private partnerships, it also encourages the involvement of public competent authorities.

Second, Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, also establishes mechanisms aimed at enhancing financial intelligence circulation. Specifically, it grants financial intelligence units (FIUs) two key powers. Article 25 of the directive introduces the possibility of issuing instructions to monitor transactions or activities, enabling surveillance of individuals posing a significant risk of money laundering or terrorist financing. Meanwhile, Article 26 allows FIUs to disclose alerts to obliged entities —providing them with relevant information to support their compliance efforts.

A common feature of these two mechanisms is that information exchange now extends far beyond typologies; it also (and above all) facilitates the sharing of personal data. EU law now fully recognises that financial intelligence must circulate more freely to enhance the effectiveness of the AML/CTF framework. However, Member States and the private sector retain significant discretion in implementing these new powers. The practical application of these various forms of cooperation among stakeholders involved in AML/CTF efforts must be closely monitored to assess the innovative approaches that may emerge across different countries and sectors.

Maxime Lassalle, Associate Professor at the University of Burgundy

BEYOND LEGAL REFORMS: WHAT REALLY SHAPES INFORMATION SHARING IN AML?

Diana Bociga Gelvez

In January 2025, Australia introduced amendments to Section 123 of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act), revising the 'tipping off' provisions. Effective from March 2025, these changes aim to facilitate better information sharing by refining prohibitions on disclosing certain details related to Suspicious Matter Reports (SMRs).

Previously, reporting entities risked criminal liability for disclosing information that could indicate the submission of an SMR to AUSTRAC or the requirement to provide information to law enforcement agencies. The law left little room for flexibility, restricting information sharing even in cases where it could have strengthened financial crime prevention. The revised law defines these restrictions more narrowly, prohibiting disclosures only when they could reasonably be expected to prejudice an investigation into an offence or proceedings related to the proceeds of crime. In theory, this change should prevent harmful disclosures while allowing reporting entities greater flexibility to share intelligence with third parties, such as auditors, consultants, or financial institutions, without breaching the law.

Undoubtedly, these legislative reforms are well-intended. Yet, laws are only one piece of the puzzle. Research on the AML regime in the UK has shown that information sharing is shaped as much by organisational culture, resource constraints, and coordination challenges as it is by legal frameworks. While AML regimes vary across jurisdictions, some of these structural and cultural barriers may also be present elsewhere, including in Australia. Without addressing these broader systemic issues, even the most well-intended legal reforms risk falling short of their objectives.

The persistent issue of resources

Information is meaningless if agencies lack the capacity to process, analyse, and act on it. Despite receiving vast amounts of data, law enforcement agencies underutilise much of it due to inadequate investment in technology, skilled personnel, and analytical capabilities. While machine learning and AI offer promising solutions for detecting financial crime patterns, these tools remain underutilised, particularly within law enforcement. Technology is only part of the problem, there is also a shortage of trained analysts who can extract meaningful insights from the data.

Cultural roadblocks

Beyond resource constraints, organisational culture remains a significant barrier to information sharing. Despite growing recognition of the need for cooperation, mistrust and secrecy still shape interactions between public and private organisations. Many law enforcement agencies hesitate to share operational intelligence, citing confidentiality concerns and legal risks. Meanwhile, private sector actors —though increasingly open to collaboration—often adopt a cautious, compliance-driven approach, sharing only what is legally required rather than proactively exchanging intelligence. A key concern is the one-way flow of intelligence, with little feedback provided to reporting entities.

Even when information is shared, it is often personality-driven rather than institutionalised. Many intelligence-sharing practices rely on personal relationships between key individuals, meaning that when they leave, trust and informal channels disappear, creating gaps in cooperation. Without strong, formalised mechanisms, intelligence sharing remains fragile and dependent on individuals rather than institutional commitments. A further complication is the interpretation of legal frameworks, which varies widely across private sector institutions. Some financial institutions take an overly restrictive approach, while others are more open, leveraging legal gateways for broader information sharing. This lack of standardisation in interpreting the law leads to fragmented practices, where the extent of information sharing depends more on internal risk appetites than on clear legal guidance.

Lack of coordination and leadership

The AML landscape is highly fragmented, with multiple public and private actors operating across different sectors, each with its own mandates, priorities, and resource constraints. There is often little alignment between these institutions, creating inefficiencies, with different entities working in silos, leading to duplication of efforts and regulatory gaps. A central challenge is the absence of a strong, empowered coordinating body to ensure that information sharing translates into meaningful action. Without a clear coordinating agency, AML responses tend to be reactive rather than proactive, driven by immediate results rather than strategic, long-term planning.

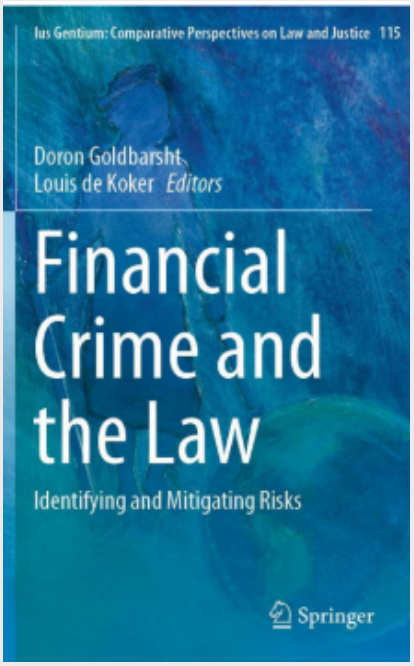
What needs to change?

Legal reforms matter, but they will not solve AML information-sharing challenges on their own. Without serious investment in technology and human resources, clearer legal guidance, a shift in organisational culture towards reciprocity, and stronger central coordination, information sharing will remain slow, fragmented, and largely ineffective. Policymakers and regulators must go beyond merely removing legal barriers and focus on the deeper structural and cultural challenges that have long impeded meaningful information sharing.

Diana Bociga, PhD Criminology candidate, University of Manchester

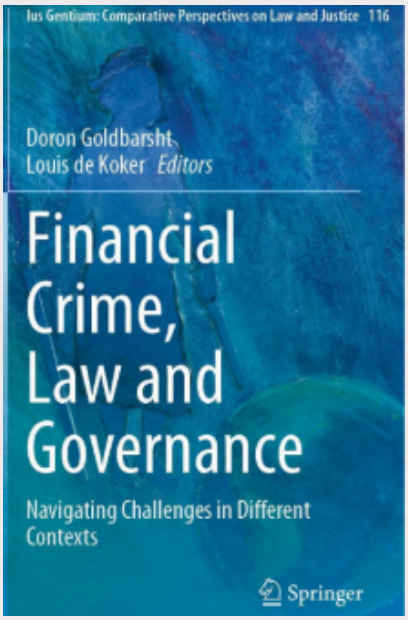
RESEARCH AT FIH

Financial Crime and the Law: Identifying and Mitigating Risks



Edited by Doron Goldbarsht and Louis De Koker, this collection explores financial crimes like crypto crime, terrorist financing, and money laundering. It offers insights into risk-based compliance, challenges in regulating weapons of mass destruction financing, and the connection between cannabis regulation and money laundering. The book also critiques the effectiveness of the risk-based approach, highlighting concerns about bias and the role of Financial Action Task Force (FATF). Essential for professionals and scholars, it deepens understanding of the complexities in financial crime risk management.

Financial Crime, Law and Governance: Navigating Challenges in Different Contexts



Edited by Doron Goldbarsht and Louis De Koker, this collection was curated by leading researchers to explore the dynamic landscape of global financial crime. It offers profound insights into the nuanced world of financial crime across diverse jurisdictions including Australia, Germany, New Zealand, Nigeria and the United Kingdom. While global standards on financial crime have solidified over the past three decades, the future direction of standard-setting and compliance enforcement remains uncertain in the complex global political landscape.

RESEARCH AT FIH

Australia's Financial Integrity: A Global Compliance Approach to AML/CTF

Co-authored by Doron Goldbarsht and Isabelle Nicolas, this book provides readers with a comprehensive understanding of the measures adopted by Australia to address global anti-money laundering and counter-terrorism financing standards set by the Financial Action Task Force (FATF). The book is structured in a way that reflects and aligns with the global standards set out by the Financial Action Task Force (FATF). Each chapter helpfully adopts the title of one of the FATF's 40 recommendations, including those recommendations and their interpretive notes, followed by questions and answers. This book's unique structure breaks down complex research findings into simple, digestible insights for practitioners and students.

FIH PODCAST

Listen to us on Spotify!

Season 2 of the *Financial Integrity Hub (FIH) Podcast*

The Financial Integrity Hub hosts regular podcasts, featuring speakers with financial crime and compliance expertise. Each podcast involves an interview with a global or local expert, allowing the Financial Integrity Hub to harness critical voices and ensure the Financial Crime community can stay up-to-date on the latest AML/CTF challenges and trends.

Episode 1 - Perspectives on AML/CTF and Risks with global experts: In celebration of the release of our new book 'Financial Crime and the Law: Identifying and Mitigating Risks', the FIH hosted a webinar where our audience had the privilege of hearing insights from renowned global experts, Dr Rachel Southworth, Prof Michael Levi, Prof Louis De Koker, and Charles Littrell.

Episode 2- Risk Management in Casinos with Armina Antoniou (Chief Risk Officer, Crown Resorts & FIH Advisory Board): Listeners can hear about Armina's approach to risk management, her view on what makes a strong risk culture, and more! Armina has approximately 20 years of experience as a risk and legal professional across Australian and global companies.

Episode 3 - Financial & Environmental Crime with Davyth Stewart: In this episode, Dr Hannah Harris interviews Davyth Stewart on the intersection of financial and environmental crime, where he provides valuable insights into key issues such as illegal logging and trade, corporate crime and trade-based money laundering.

Thank you to our podcast partner - CFCE!

CFCE sets itself apart as an exceptional AML/CTF course provider with a unique focus on the Australian industry. What makes CFCE even more appealing is that these valuable educational opportunities are not only highly informative but also cost-effective.

CFCE
CERTIFIED FINANCIAL CRIME EXPERTS

CFCE offers 50% discounts to FIH readers: Fundamentals in AML, Fundamentals in CTF, AML/CTF for Clubs and Pubs, KYC, CDD, and others. Just use the code "CFCE-FIH". Contact: office@cfce.com.au

UPCOMING FIH EVENTS

Integrity Insight: Financial Crime Summit

Join us for a full day of in-depth discussions on AML/CTF/CPF, fraud, sanctions, and more. Together, we'll explore the latest trends, emerging threats, and effective mitigation strategies. Whether you're a seasoned professional, regulatory expert, or academic researcher, Integrity Insight offers valuable insights and unmatched networking opportunities.

👉 Registration: Click HERE, or Scan:

RECENT FIH EVENTS

THE “FINANCIAL WAR ON CRIME AND TERRORISM" SEMINAR SERIES

Innovations in Financial Crime: Opportunities and Challenges

Speakers for this event included

- **Michael Brand, Louis de Koker, and Carl Herse** - Privacy-preserving data analytics: A case study in AML/CTF innovation in Australia
- **Paula Chadderton** - FATF and the public-private sector information-sharing conundrum
- **Doron Goldbarsht and Timothy Goodrick** - Private to Private: The Next Frontier of Financial Intelligence Sharing
- **Milind Tiwari** - Network analytics and Generative AI: A hybrid approach to money laundering detection

Financial Crime, Corruption, and the Power of Leadership

Speakers for this event included:

- **Jeffrey Simser** - Dangerous Play: AML/CTF/CPF Risks in the Gaming Sector
- **Petrus C. van Duyne and Jackie Harvey** - Corrupt elites and godfathers in Nigeria
- **Michelle Gallant** - Unexplained Wealth Orders: Surveying the Rights-Based Landscape
- **Nick Donaldson and Christian Leuprecht** - Corruption Without Borders: Transnational Patterns of State Capture
- **Robert Walters** - International Arbitration and Money Laundering: Is there an actual issue?

Counter-Terrorism, Human and Environmental Rights

Speakers for this event included:

- **Jeffrey Simser -** Dangerous Play: AML/CTF/CPF Risks in the Gaming Sector
- **Nick Donaldson and Christian Leuprecht** - Corruption Without Borders: Transnational Patterns of State Capture
- **Rachel Southworth and Jamie Ferrill** - Beyond Compliance: The Role of Leadership and Culture in Combatting Financial Crime.
- **Vivienne Lawack -** CBDCs, Financial Inclusion, and Financial Integrity: Trade-Off?

Financial Crime, National Security, and Safeguarding Society

Speakers for this event included:

- **Ben Scott** - Deception in money laundering
- **Sanaa Ahmed** - Surveilling the citizen: Crime control policies, national security discourses, and money laundering regulation in Canada
- **Megan Styles** - De-banking 'risky' customers: Contractual exclusion of customers by financial institutions and AML/CTF ramifications
- **Derwent Coshott** - Challenging Risk: The Case of Maples Corporate Services v CIMA.

WORK WITH US

The Financial Integrity Hub (FIH) relies on a network of experts across business, government and higher education. It promotes an interdisciplinary understanding of financial crime by bringing together perspectives from the fields of law, policy, security, intelligence, business, technology and psychology.

The FIH offers a range of services and collaborative opportunities. These include professional education, hosting events to promote up-to-date knowledge, publishing key insights and updates, and working with partners on their business challenges.

If your organisation would benefit from being part of a cross-sector network and having a greater understanding of the complex issues surrounding financial crime, please contact us to discuss opportunities for collaboration: fih@mq.edu.au.

If you would like to contribute your op-ed for our future FIH Insights, please contact us.