

FIH INSIGHTS

From Collaboration to Collective Disruption

Follow the Data, Follow the Money

When Information Moves, But
Accountability Doesn't

P2P
Information
Sharing &
Beyond

JODIE ARTHUR

LEADERSHIP

Patron

Hon. Patricia Bergin AO SC

Director

Associate Professor Doron Goldbarsht

Associate Director

Isabelle Nicolas

Distinguished Fellows

Professor Christian Leuprecht

David Lewis FRGS

Professor Nicholas Ryder

Advisory Board

Armina Antoniou

Joanna Bird

Professor Louis De Koker

Paul Jevtovic APM OAM

Professor Elizabeth Sheedy

Michael Tooma

Stuart Clark AM (d. June 2025)

Reference Group

Sue Bradford

Gail Carter

Claudine Lamond

Jeremy Moller

Research Fellows

Professor Sean Foley

Dr Mirella Atherton

Dr Daley Birkett

Dr Derwent Coshott

Dr Jamie Ferrill

Dr Hannah Harris

Dr Jeanne Nel

Dr Milind Tiwari

Researchers

Shehnika Iqbal

Giang Nguyen

Isabelle Nicolas

Samuel Orchard

Ben Scott

Chief Editor, FIH Insights

Reem Armano

Interns

Patricia Motahari

Madeleine Olney

Sara Torrisi

Lucas Tulich

Citing reference: Financial Integrity Hub 'FIH Insights' (2026) 3(3) FIH, Sydney
<<https://www.mq.edu.au/research/research-centres-groups-and-facilities/groups/financial-integrity-hub/engagement>>.

Featured on the cover, General Manager, Financial Crime and Group AMLCO, Westpac Banking Group, Jodie Arthur.

ABOUT US



The Financial Integrity Hub (FIH) is a leading research centre 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:



**FINANCIAL
INTEGRITY HUB**



MACQUARIE
University
SYDNEY-AUSTRALIA



TABLE OF CONTENTS

From the Editor

Interview with Jodie Arthur

Opinion Pieces

From Takedowns to Information Sharing: Rethinking the Fight Against Cryptocurrency Mixers in Money Laundering

Wesley Kwan & Christian Leuprecht

From Collaboration to Collective Disruption

Jodie Arthur

Private-to-Private Information Sharing in Relation to Payment Fraud in France and Europe

Maxime Lassalle-Han

Role of Public-Private Partnerships in the Effectiveness of AML/CFT Systems: Evidence from India's FPAC and ARIFAC

Smarak Swain

Challenges, Considerations and Barriers to Effective Public-to-Private Information Sharing

Rachel Waldren

Disrupting Financial Crime Through Private-to-Private Information Sharing

Ben Scott

Lessons from Established Information Sharing Models for Public-Private Partnerships in Australia and Internationally

Paula Chadderton

From Social Networks to Financial Networks: The Emerging Terrorist Financing Challenge and Why Collaboration is the Key Defence

Nadine Jones

Integrating the Purpose Limitation and Fishing Expedition Prohibition Principles in the Implementation of Public-Private Partnership in the AML/CFT Regime

Go Lisanawati

Neither Sharing nor Protection: Why Data Protection Law Misses AML Data Processing

Umay Şener

Follow the Data, Follow the Money: Strengthening the Link Between Cyber Incident Reporting and Financial Crime

Ha Do

When Information Moves, But Accountability Doesn't

Adam Famao

FIH Research

FIH Podcasts

FinCrime & Culture

Financial Crime Files

FIH Events

P2P
Information
Sharing &
Beyond

FROM INFORMATION TO ACTION: RETHINKING FINANCIAL INTELLIGENCE SHARING



Image: Prof Louis de Koker at the 2026 Financial Integrity Week Intelligence Sharing Panel.

As financial systems become more digital, interconnected and complex, no single organisation is likely to possess the complete picture of a transaction, customer or criminal network. Bringing together different sources of intelligence, expertise and insight can help reveal connections and patterns that might otherwise remain hidden. Information sharing is therefore an increasingly important component of the global response to money laundering, terrorist financing and other forms of financial crime; but its value lies not simply in the volume of information exchanged. Information must reach the right people, at the right time, and in a form that can be meaningfully analysed and acted upon.

Achieving this is not without challenges. Effective information sharing raises difficult questions. What information can be shared, by whom and for what purpose? What legal gateways and safeguards are required? How can privacy, confidentiality and data protection obligations be respected while still enabling timely intervention? And how can information sharing be expanded beyond traditional relationships between financial institutions and government?

Beyond Public-to-Private Information Sharing

Public-Private Partnerships (PPPs) are increasingly recognised as an effective means of mitigating financial crime risks, enabling a shift from predominantly reactive and compliance-driven approaches towards more proactive and collaborative responses. By bringing together information, resources, technology and specialised expertise from across the public and private sectors, PPPs can generate insights and capabilities that may not otherwise be available to any single agency or organisation.

The flow of information, however, does not have to be one-directional. Public authorities can provide the private sector with intelligence about emerging threats, typologies, risk indicators and criminal methodologies, while reporting entities and other private-sector organisations should contribute information derived from their own customer relationships, transaction monitoring and operational experience. There is also value in private-to-private information sharing, which offers opportunities for more preventative and coordinated responses to illicit finance.



Image: David Lewis, Jon Brewer, and Brett James at the 2026 Financial Integrity Week Intelligence Sharing Panel.

Banks, payment providers, virtual asset service providers (VASPs), professional services firms, and digital platforms may each hold different pieces of the same financial crime puzzle. Greater collaboration between private-sector organisations can enable risks to be identified earlier and understood more comprehensively.

This broader conception of information sharing is particularly important as criminal activity becomes increasingly networked. Fraud, money laundering, cybercrime and other forms of illicit finance can move across sectors and platforms at the speed of the internet. Information-sharing frameworks therefore need to evolve alongside the methods used by those seeking to exploit the financial system.

A Global Shift Towards Collaboration

The growing international focus on information sharing is reflected in the Financial Action Task Force's (FATF) July 2026 report, *Information Sharing to Combat Illicit Finance: Global Overview of Public and Private Sector Partnerships and Data Protection Arrangements*. The report examines how public-private partnerships and other information-sharing arrangements are being used across jurisdictions to strengthen the detection and disruption of money laundering, terrorist financing and proliferation financing.

The scale of these arrangements is significant. The FATF identified at least 84 PPPs globally, with 52 surveyed jurisdictions reporting at least one domestic partnership and 18 reporting more than one. Its findings suggest that PPPs can provide an enduring mechanism for combating illicit finance when supported by appropriate legal foundations, clear governance arrangements and technological capability.

The report also points towards a broader information-sharing ecosystem. Alongside financial institutions and government authorities, there is increasing scope for VASPs, non-financial sectors and other non-traditional stakeholders to contribute to the collective response to financial crime. Technological developments, including encrypted platforms and secure information exchanges, are further changing how information can be shared.

The message is therefore not simply that more information should be exchanged. Rather, effective information sharing depends on the frameworks

surrounding that exchange, including legal authority, governance, data protection, security and the appropriate use of technology.

Fintel Alliance: An Australian Example

Australia provides a notable example of this approach through AUSTRAC's Fintel Alliance. Established in 2017, Fintel Alliance brings together government, law enforcement and private-sector partners to share and analyse financial intelligence, and develop responses to serious and emerging financial crime threats. Its partners have included major banks, remittance providers, gambling operators and law enforcement and government agencies. The model illustrates how information sharing can move beyond conventional reporting relationships.

Fintel Alliance provides a setting in which public and private partners can combine their respective data, expertise and capabilities to identify threats, develop intelligence and support disruption activity. The initiative has also continued to evolve. In 2025, AUSTRAC expanded Fintel Alliance, with the Collaborative Analytics Hub becoming a central function and an increased focus on closer to real-time analysis and collaborative intelligence. As new sectors come within the scope of AML/CTF obligations following the Reforms, a key challenge will be ensuring that information-sharing arrangements facilitate timely and meaningful collaboration while preserving appropriate protections for privacy, confidentiality, and commercially sensitive information.

In this Edition

The question facing policymakers, regulators, law enforcement and industry is therefore not simply whether information can be shared, but whether existing frameworks enable it to be shared effectively, responsibly and at the speed required to respond to modern financial crime. This edition of *FIH Insights* explores that question through the legal and regulatory frameworks, public-private partnerships, private-sector collaboration and safeguards that shape effective information sharing.

As financial crime continues to evolve across borders, sectors and technologies, breaking down information silos will remain essential to strengthening prevention, detection and disruption, and ultimately safeguarding the integrity of the financial system.

INTERVIEW WITH JODIE ARTHUR

GENERAL MANAGER, FINANCIAL CRIME AND GROUP AMLCO | WESTPAC BANKING GROUP



My Professional Journey

My career in financial crime has been shaped by risk management, regulatory engagement, international experience, and a clear sense of purpose. I began my career in Audit, which gave me exposure to a wide range of business lines, both within and beyond financial services. That experience gave me a strong grounding in governance, controls, and organisational complexity. I then moved into senior risk and compliance roles across banking, including financial crime leadership roles with ANZ in Australia and Singapore, and Standard Chartered across ASEAN and South Asia. Those roles exposed me to multi-jurisdictional AML/CTF, sanctions, fraud, and anti-bribery and corruption risks, and reinforced the importance of frameworks that are both globally consistent and locally effective. Across each of these roles, the same lesson has stood out: financial crime cannot be disrupted effectively by any one institution acting alone.

I joined Westpac in 2020 as Head of Financial Crime Compliance for the Consumer and Business division and was appointed General Manager, Financial Crime and Group MLRO in 2023. Today, I lead Westpac's group-wide approach to financial crime risk management, including AML/CTF, sanctions, bribery and corruption, tax transparency, fraud and scams, and related risks. I also act as the AML/CTF Compliance Officer under AUSTRAC legislation and manage key regulatory relationships in Australia and internationally.

“What keeps me committed to this work is its connection to real-world harm: scams, fraud, organised crime, exploitation, and national security threats. Helping disrupt that harm, while strengthening trust in the financial system, is both a responsibility, and a privilege.”

What are your thoughts on information sharing and the future of collaboration from the perspective of a major financial institution?

For a major financial institution, it is one of the most important levers for improving the collective response to financial crime. Banks see significant volumes of activity and can identify patterns across customers, products, and channels. But each institution sees only part of the picture. Government agencies, law enforcement, regulators, and the private sector each hold different pieces of intelligence. The value comes when those pieces can be brought together lawfully, safely, and with clear purpose.

In my experience, public-private collaboration is most effective when it is threat-led and outcome-focused. The Fintel Alliance has demonstrated the value of bringing AUSTRAC, law enforcement, and reporting entities together to develop shared intelligence, identify emerging typologies, and support disruption activity. At its best, information sharing enables earlier identification of criminal networks, more targeted suspicious matter reporting, better intelligence for law enforcement, and more informed risk management across industry.

The next phase of collaboration needs to move beyond periodic or case-by-case exchanges toward more structured, scalable, and near-real-time intelligence sharing. That does not mean sharing everything with everyone. It means creating trusted environments supported by strong governance, privacy and legal safeguards, common data standards, and clear escalation pathways, so that relevant intelligence can be used responsibly and quickly. It also means shifting

from a primarily prevention-based mindset to one that gives greater weight to disruption: identifying the networks, behaviours, and vulnerabilities criminals exploit, and acting collectively to reduce their ability to move funds through the system.

“Responding effectively to financial crime requires more than strong controls within individual institutions; it requires trusted collaboration across government, law enforcement, regulators, and industry. For me, that purpose — protecting customers, communities, and the integrity of the financial system — has been a consistent thread throughout my career.”

What are some challenges and opportunities for collaboration between government, regulators, law enforcement, and the private sector?

The case for collaboration is clear, but the barriers are real. A key challenge is that the financial crime ecosystem remains fragmented, while criminal networks are not. Criminals exploit gaps between institutions, sectors, borders, and legal frameworks. They move quickly, use technology effectively, and adapt when controls improve. Legitimate information sharing, by contrast, must operate within legal, privacy, secrecy, operational, and conduct obligations. Those safeguards are essential, but collaboration can become slower and more complex when roles, permissions, and thresholds are unclear.

Trust is another critical factor. Collaboration depends on confidence that shared information will be used for the right purpose, protected appropriately, and translated into action. It also requires a shared understanding of risk appetite and operational constraints. Financial institutions need to act on intelligence in a way that is proportionate and defensible, while regulators and law enforcement need information that is timely, specific, and actionable. That mutual understanding is built through sustained engagement, not just formal mechanisms.

The opportunity is to move from institution-by-institution compliance to a more system-wide response.

Better collaboration can support earlier sharing of typologies, faster identification of mule networks and organised fraud rings, stronger reporting to AUSTRAC, and more useful intelligence for law enforcement. It can also help newly regulated sectors lift capability through practical indicators, guidance, and shared learning. As Australia’s AML/CTF regime expands and modernises, collaboration will be critical to improving outcomes rather than simply adding process.

What do you think are some emerging trends and priorities for information sharing in Australia’s AML/CTF framework?

Against that backdrop, several priorities are emerging for information sharing in Australia’s AML/CTF framework. The first is timeliness. Threats such as scams, mule activity, fraud, illicit tobacco, child exploitation, sanctions evasion, and organised money laundering evolve quickly. Intelligence has the greatest impact when it helps institutions detect activity earlier, supports law enforcement disruption, or prevents further harm to customers and the community.

The second priority is collaborative analytics. Shared data, advanced analytics, and network detection can reveal patterns no single institution can see alone. This will become increasingly important as criminal activity becomes more digital, dispersed, and sophisticated. The challenge is to ensure these capabilities are supported by strong governance, explainability, auditability, and privacy controls, so innovation strengthens both effectiveness and public trust.

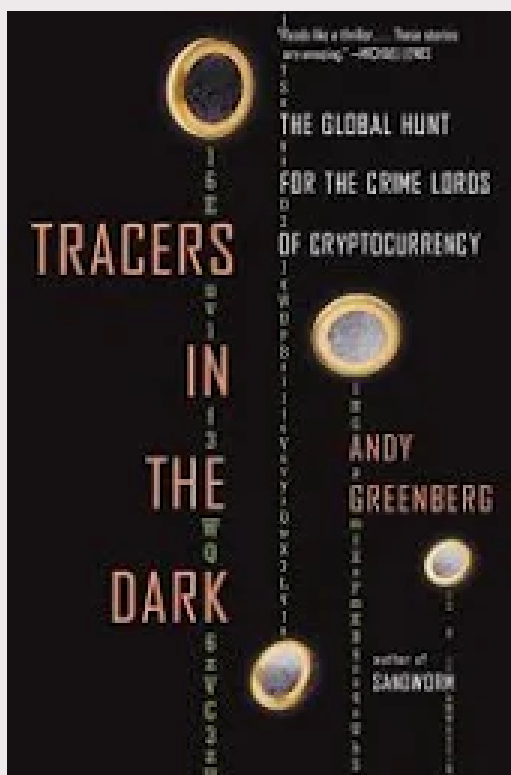
The third priority is legislative clarity. Reforms to tipping-off provisions and the broader AML/CTF regime can reduce unnecessary barriers to responsible collaboration while maintaining safeguards that protect investigations and customer information. As the regime expands to additional sectors, cross-sector intelligence will become more important in following suspicious activity beyond banks and into professional services, real estate, digital assets, and other areas criminals may seek to exploit.

Ultimately, the focus must remain on outcomes. The measure of effective information sharing is not the volume of data exchanged, but whether it improves detection, strengthens reporting, supports disruption, reduces harm, and helps build a more resilient financial system.

Finally, is there a relevant book, article, film, or podcast you would recommend to our audience, and why?

For readers interested in the broader context of financial crime, I recommend *Tracers in the Dark* by Andy Greenberg. It is a compelling account of how investigators used blockchain analytics to trace illicit funds through cryptocurrency networks and dismantle major criminal marketplaces. For financial crime professionals, it is a timely reminder that technology can create new vulnerabilities, but also new opportunities for intelligence-led disruption.

In a similar vein, I would also recommend the ABC series *Capture*, which explores the use of deepfakes and deception in a government context. It reinforces how quickly technology-enabled threats are evolving, and why financial crime professionals need to keep looking beyond traditional risk indicators.



“The broader lesson is that collaboration is no longer optional in financial crime risk management. No single institution, agency, or regulator can see the whole picture alone. The next phase of maturity will depend on combining strong governance with practical action and using shared intelligence to detect, disrupt, and prevent harm at scale.”

FROM TAKEDOWNS TO INFORMATION SHARING: RETHINKING THE FIGHT AGAINST CRYPTOCURRENCY MIXERS IN MONEY LAUNDERING



Wesley Kwan | Researcher, Institute of Intergovernmental Relations, Queen's University, Canada | JD Candidate, Columbia Law School
Dr Christian Leuprecht | Professor, Royal Military College of Canada and Queen's University, Canada | Distinguished Fellow, Financial Integrity Hub

Over the past decade, cryptocurrency mixers have undermined traditional anti-money laundering (AML) approaches in fighting crypto-laundering. Operating on the assumption that solving money laundering meant nullifying the responsible criminal entity, authorities have spent most of their efforts on a wild goose chase identifying, sanctioning, and/or taking down cryptocurrency mixers. While law enforcement has seen some successes, the decentralised nature of mixers has led them to be uniquely resilient against AML action. Disruption of one service merely displaces illicit activity toward another.

Our study, “Crypto-Crime Tumblers: Criminogenic Attributes of Cryptocurrency Mixers in Enabling Financial Crime and Money Laundering,” examines 32 mixer-related court cases. The aim is to identify patterns in the way crypto-launderers operate, and opportunities for targeted AML enforcement.

“Our analysis finds crypto-laundering by way of mixers to be highly concentrated: five mixers were responsible for over \$6 billion transferred in illicit cryptocurrency. Tornado Cash alone laundered over \$2.2 billion from illegal sources.”

Furthermore, crypto-launderers frequently take advantage of decentralised services: non-custodial mixers have transferred over \$9 billion in cryptocurrency (custodial services transferred \$8.3 billion in total). Of note, only 3 out of 14 analysed mixers were non-custodial. Additionally, crypto-laundering with mixers is highly networked.

Crypto-launderers involve many different actors: *overseers* operate mixers, *personal users* use existing mixers to conceal their own criminal proceeds, and *enablers* facilitate crypto-laundering by operating exchanges or other services with deficient AML or know-your-customer (KYC) controls. That typology changes our appreciation of crypto-laundering: instead of an isolated laundering machine, mixers are one component in a chain that involves criminals, wallets, exchanges, and ultimately institutions through which value can be converted, transferred, or integrated.

Current AML strategies focus on mixer takedowns, which yield a temporary fix rather than a sustainable solution. For instance, when Tornado Cash faced sanctions in 2022, transaction volumes dropped around 72%. Subsequently transaction volumes dropped by 90% when its web-based interface was taken down.

However, crypto-launderers such as Lazarus Group, a North Korean cyber hacking group, simply transitioned to alternative mixers that quickly filled the gap, such as Sinbad.io and later YoMix. Enforcement measures notwithstanding, Tornado Cash would experience a resurgence, with a 108% year-over-year increase in cryptocurrency inflow in 2024.

In March 2025, Tornado Cash's sanctions were finally removed over legal challenges to the government's latitude to sanction decentralised protocols. Evidently, reactive AML strategies do not fare well against mixers. Decentralised services have no central operator to arrest, no corporate office to raid, and no central database to seize. When law enforcement disrupts a mixer, another takes its place and crypto-launderers merely substitute services.

Accordingly, authorities must substitute proactive strategies for reactive AML strategies to address mixers and crypto-laundering more effectively.

Information sharing is key to informing such a proactive strategy. Crypto-laundering networks do not operate within a single institution or jurisdiction, and neither does the information needed to detect them. Law enforcement may possess intelligence on known criminal actors, illicit wallet addresses, sanctioned entities, and suspicious behavioural patterns. Cryptocurrency exchanges and other virtual asset service providers (VASPs), meanwhile, may store customer identification records, wallet attribution data, and transaction histories.

Banks may observe deposits, withdrawals, account relationships, and other activity as crypto is converted into fiat currency. Blockchain analytics firms can identify patterns in the movement of funds across otherwise pseudonymous addresses. Individually, these actors may see only part of a laundering scheme. Collectively, they can reconstruct the criminal network, allowing authorities to identify vulnerable areas to target with proactive AML regulation.

The criminal case of *Ilya Lichtenstein and Heather Morgan* demonstrates the value of connecting information across this broader ecosystem. According to US prosecutors, Lichtenstein stole \$71 million worth of Bitcoin from a major cryptocurrency exchange. Using mixers, Lichtenstein and Morgan then hid their illicit funds by transferring them across different cryptocurrency wallets, darknet market accounts, and 10 different cryptocurrency exchange accounts. They also used fictitious identities to create accounts at exchanges and converted Bitcoin into altcoins, including privacy coins. The pair were only caught more than five years later, when investigators combined with blockchain analysts to trace stolen funds to an account linked with Lichtenstein's real identity.

“Lichtenstein’s case, solved with public-private information sharing, highlights that crypto-launderers and mixers do not operate in isolation from the legitimate financial system.”

Exchanges remain particularly important at the beginning and end of crypto-laundering chains, where criminals acquire cryptocurrency, transfer assets between services, and eventually convert digital assets into fiat currency. Even when a decentralised mixer itself is difficult to regulate, its users frequently interact with centralised entities that are subject to AML/KYC requirements.

Although mixers can obscure the transaction trail, criminals still leave fragments of information across multiple public and private institutions. AML policy objectives should, therefore, extend beyond identifying and dismantling mixers to identifying regulated gateways through which illicit funds ultimately flow. Information sharing can transform these gateways from passive intermediaries into active points of detection and disruption.

“Ergo, effective public-to-private information sharing goes beyond circulating lists of sanctioned entities after enforcement action has already occurred.

Rather than prosecuting financial institutions and VASPs after they become entrenched in laundering networks, authorities should proactively share emerging indicators of illicit activity, such as high-risk wallet addresses, newly identified mixer infrastructure, transaction typologies, and patterns associated with known criminal groups. ”

Just as importantly, information must flow in both directions. Usually private-sector institutions are closest to observing unusual transaction patterns, interaction with newly emerging services, or attempts to move funds into the conventional financial system. Rapidly feeding that information back to financial intelligence units and law enforcement enables authorities to identify emergent laundering methods before they mature into large-scale criminal infrastructure.

Proactive efforts to apply such AML/KYC policies to cryptocurrency exchanges and mixers notwithstanding, non-compliance by Binance and BTC-e suggests that the efficacy of such efforts is limited. For one, jurisdictional regulatory arbitrage allows non-compliant services to set up in countries with weak oversight: as of June 2025, 27% of countries had not implemented requirements for VASPs to obtain and disclose sender/recipient information for cryptocurrency transactions.

For cryptocurrency exchanges or mixers to comply with governmental regulations, they will have to be incentivised such that the risk of not doing so (or benefit of doing so) outweighs the value of upholding their cryptoanarchist philosophy, which champions privacy and is deeply skeptical of centralised authority and law enforcement. Arrests and prosecutions may deter some, but AML experts will need to find better incentives to contain the proliferation of non-compliant mixers and exchanges.

Not every use of a cryptocurrency mixer is evidence of criminality or justifies indiscriminate surveillance of cryptocurrency users. Indeed, mixers can serve legitimate privacy interests.

“Excessive information sharing risks undermining the very financial privacy that decentralised technologies were designed in part to preserve (while also legitimising cryptoanarchist ideologues).”

Ergo, the goal should be to foster the timely exchange of strategic intelligence to identify patterns associated with serious financial crime, within clear legal authorities, proportionality safeguards, and defined AML objectives. By actioning proactive information sharing over reactive takedowns, authorities will find themselves freed from their expensive, perpetual, and ineffective game of “whack-a-mixer.”

Based on the authors’ forthcoming article in the Journal of Contemporary Criminal Justice entitled “Crypto-Crime Tumblers: Criminogenic Attributes of Cryptocurrency Mixers in Enabling Financial Crime and Money Laundering”.

Wesley Kwan & Christian Leuprecht

FROM COLLABORATION TO COLLECTIVE DISRUPTION



Jodie Arthur | General Manager, Financial Crime, Westpac, Australia

Financial crime is no longer a threat any one institution, agency or sector can tackle alone. As criminal networks become faster, more sophisticated and increasingly borderless, our response must become more connected, intelligence-led and action-oriented. Public-to-private information sharing has an important role to play. Its real value lies not in sharing more information, but in turning the right intelligence into earlier prevention, coordinated disruption and reduced harm.

Financial crime threats are pervasive and borderless. The criminal economy is decentralised, franchised and fast-moving; it is also agile, sophisticated and increasingly innovative in how it exploits gaps between sectors, jurisdictions and technologies. In an increasingly digital payments landscape, that speed and opacity make isolated institutional responses less effective and increase the need for timely intelligence across the full value chain.

Regulation has rightly placed significant obligations on banks and the broader financial services sector. But if we continue to treat the largest institutions as the primary line of defence, we will miss the wider value chain criminals exploit: technology platforms, payment intermediaries, professional enablers, digital assets and crypto channels, remitters and cross-border networks. The equation is incomplete unless the whole ecosystem is part of the response.

When larger institutions harden their controls, criminal activity does not disappear; it moves to less mature, less visible or less connected parts of the system. Without broader information sharing, risk is displaced rather than disrupted. Public and private sector collaboration is no longer optional; it is the operating condition for preventing harm, disrupting criminal networks and protecting the integrity of the financial system.

The economic case for stronger public-to-private and private-to-private information sharing is compelling. In 2025, the Australian Institute of Criminology estimated serious and organised crime in Australia to cost up to A\$82.3 billion a year (around 3.2% of GDP), with organised financial crime alone accounting for A\$13.2 billion in direct costs.

Globally, the scale is even more confronting. The United Nations Office on Drugs and Crime estimates that money laundering represents 2-5% of global GDP each year, while more recent private-sector analysis places the figure at around US\$5.5 trillion annually. These figures underline a simple reality: financial crime is not a marginal compliance issue; it is a systemic economic threat that requires a system-wide response.

So where to from here? The next phase must move beyond goodwill, forums and information exchange as ends in themselves.

“Public-private partnerships need to become operating models for prevention, structured around shared priorities, trusted intelligence pathways, clear legal guardrails, and measurable disruption outcomes.”

Information sharing should not be treated as a solution in itself. More data, alerts and forums will not necessarily translate into better prevention outcomes. Without clear priorities, legal safeguards, disciplined governance and operational accountability, sharing can create noise rather than insight. Globally, public-private partnership models have demonstrated their value, but the next challenge is maturity.

The question is no longer whether collaboration matters; it is whether partnerships are evolving fast enough to match the threat. To move to the next stage, they must become more intelligence-led, data-enabled, strategically focused and judged by their ability to prevent harm and disrupt criminal activity.

“The real test is whether the right intelligence reaches the right decision-makers early enough to prevent harm.”

Partnerships should be judged by practical impact: timely, actionable intelligence that is translated into operational decisions. Success should then be measured across three connected outcomes: prevention, detection and disruption. Prevention asks whether intelligence helps institutions stop harm before it occurs. Detection asks whether shared typologies, indicators and risk signals improve the ability to identify suspicious activity earlier. Disruption asks whether collective action leads to tangible results, including impaired criminal networks, restrained or recovered funds, disrupted mule accounts and infrastructure, better targeted law enforcement activity, and fewer opportunities for criminals to exploit gaps across the ecosystem.

The recent Anti-Money Laundering and Counter-Terrorism Financing reforms are expected to provide greater scope for private-to-private information sharing, subject to supporting rules, safeguards and implementation settings that are still being finalised. Used safely and proportionately, this could shift the dial from institution-by-institution defence to collective ecosystem disruption and prevention.

Cross-border information sharing and international cooperation are also essential. Criminal networks do not organise themselves around national boundaries, and fragmented intelligence creates opportunities for funds, identities and infrastructure to move faster than the response. Effective international cooperation should therefore focus on trusted pathways for sharing priority threats, typologies and disruption opportunities across jurisdictions.

For these partnerships to drive genuine prevention and disruption, success measures need to be agreed at the outset and reviewed regularly. Activity measures such as alerts, meetings or intelligence products are useful, but insufficient. Stronger measures are outcome-based: confirmed disruption opportunities, funds restrained or recovered, criminal infrastructure identified, priority typologies mitigated, intelligence adopted into controls, and evidence that fewer customers are harmed.

Ultimately, public-private intelligence partnerships will succeed if they make the system harder for criminals to exploit and safer for the people and communities financial crime harms. That requires a disciplined operating model that turns shared intelligence into earlier intervention, coordinated disruption and measurable prevention outcomes.

We have a shared commitment to protecting the integrity of Australia’s financial crime ecosystem and to playing our part globally in hardening the system. The imperative now is to turn that commitment into measurable prevention, earlier disruption and reduced harm. This is no longer something we should aspire to do; it is something we must deliver.

Jodie Arthur

PRIVATE-TO-PRIVATE INFORMATION SHARING IN RELATION TO PAYMENT FRAUD IN FRANCE AND EUROPE



Dr Maxime Lassalle-Han | Associate Professor, University of Burgundy, Membre of the Institut Universitaire de France

In response to the rise in payment fraud, France decided to create a national database of accounts flagged for fraud risk (Law No. 2025-1058 of November 6, 2025) aimed at strengthening the fight against bank fraud. This law merely paved the way for the creation of this registry and required the adoption of regulatory provisions to enable its implementation (Decree of April 24, 2026, defining the technical operating procedures for the registry referred to in Article L. 521-6-1 of the Monetary and Financial Code).

“The purpose of this database is to centralise information that enables the identification of accounts that payment service providers deem likely to be fraudulent, based in particular on analyses conducted as part of their internal anti-fraud measures.”

Through this file, the service provider shares certain information (such as the account identifier (IBAN), the identifier of the institution holding the account, the date of detection, the origin channel of the fraudulent transaction, the source of the fraud, the category of fraud, the type of transaction, and, where applicable, the existence of a claim or complaint from a payment service user regarding identity theft) with other payment service providers. Furthermore, to prevent unsubstantiated suspicions from being disseminated on a large scale for too long, the payment service provider that adds an account to the database *“shall immediately conduct checks to assess whether the account is fraudulent and shall share the results as soon as possible in each report concerning an account it holds.”*

It should be noted that this regulatory text was adopted following an opinion issued by the national data protection authority (Decision 2026-044, April 16, 2026).

The authority expressed significant reservations regarding the operation of this database. First, a key concern for the data protection authority is that the shared data is “highly personal.” Thus, the sharing of information is likely to have significant consequences for individuals, particularly when a reported suspicion of fraud is ultimately found to be unfounded.

Second, and this is undoubtedly the most significant issue, the system’s architecture itself could pose a problem. The data protection authority criticises the large-scale sharing of data among numerous parties. According to the authority, the suspected bank credentials are shared “in plain text,” even though it would have been technically feasible to share the data confidentially.

It is also worth noting that, by adopting this legislation, France was anticipating developments in European Union law.

“An important package is in fact about to be published in the Official Journal of the European Union, a new Payment Services Regulation (PSR) and the Third Payment Services Directive (PSD3).”

This package provides, in addition to the obligations applicable to payment service providers, for the implementation of mechanisms for sharing information among providers.

The idea is that, while providers must assume certain responsibilities regarding funds lost due to bank fraud, they must also have the means to detect suspicious accounts. The French private-to-private information sharing mechanism currently addresses only the issue of payment fraud.

“However, this novelty raises the question of how it will interact with other forms of private-to-private cooperation.”

As highlighted in the European package that is about to be published in the *Official Journal*, these mechanisms will inevitably interact with two types of private-to-private partnerships. On the one hand, there are those developing in the area of combating money laundering and terrorist financing, particularly under Article 75 of *Regulation (EU) 2024/1624* of the European Parliament and of the Council of May 31, 2024, on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

On the other hand, there are the mechanisms for sharing information and intelligence on cyberthreats set forth in *Regulation (EU) 2022/2554* of December 14, 2022, on the digital operational resilience of the financial sector and amending *Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014, and (EU) 2016/1011*.

With regard to partnerships in the fight against money laundering, we know that *Regulation 2024/1624* will not take effect until July 10, 2027. The question of how the two systems will interact is therefore still premature, but it will eventually arise.

While the private-to-private information-sharing partnership currently taking shape in France is, for the time being, focused on combating payment fraud, it foreshadows future developments in the fight against money laundering and terrorist financing. The issues that have arisen in this context, particularly regarding data protection, will therefore need to be revisited.

Maxime Lassalle-Han

ROLE OF PUBLIC-PRIVATE PARTNERSHIPS IN THE EFFECTIVENESS OF AML/CFT SYSTEMS: EVIDENCE FROM INDIA'S FPAC AND ARIFAC



Smarak Swain | Director (AML/CFT Policy), Department of Revenue, Government of India | Co-Chair, Risk, Trends and Methods Working Group (RTMG), FATF

The digitalisation of the economy has significantly changed the landscape of Money Laundering (ML) & Terrorism Financing (TF) risks across jurisdictions. While traditional channels for moving money are metamorphosing, new channels have exposed us to new vulnerabilities for the movement of illicit finance. Three interlocking features of the digital economy have structurally changed the nature of the challenge AML/CFT personnel face.

First is velocity, which has become a risk multiplier. Secondly, faster cross-border transmission of value, through virtual assets and innovative fintech solutions, creates time pressure for asset tracking and recovery. Third, increasingly complex typologies, made possible by myriad fintech solutions, imply that risk understanding of key stakeholders needs to be updated more frequently.

Speed, borderlessness, and complexity imply that no single competent authority or private-sector intermediary, in isolation, possesses the complete picture needed to understand ML/TF risks.

“While collaboration has always been important for developing an effective AML/CFT system, the new reality of fragmented information has pushed it to the centre of AML/CFT policy.”

A recent Financial Action Task Force (FATF) paper on public-private partnerships (PPPs) needs to be viewed in light of this new reality. The strategic imperative to address and mitigate the emerging risks of the digitalisation of the economy lies in closer public-private partnerships (PPPs) and private-to-private (P2P) partnerships.

This article argues that PPPs serve as a force multiplier for risk understanding and risk-based response by fostering collaboration among FIUs, supervisors, and the private sector. At the same time, P2P partnerships lead to network-wide enhancement of financial integrity. It uses India's experience with PPP and P2P collaborations to highlight their utility in enhancing effectiveness across AML/CFT systems.

Public-Private Partnerships

A PPP in the AML/CFT context is a structured mechanism, usually hosted by a FIU or a supervisory authority, through which competent authorities and obliged entities exchange strategic and operational information. FATF's recent 2026 work on these arrangements surveyed numerous FATF and FATF-styled regional body members and identified more than eighty such partnerships operating across more than fifty jurisdictions, at varying stages of maturity. The overview found that strategic information sharing in the form of typologies, red-flag indicators, and risk trends is now common practice in the vast majority of surveyed jurisdictions. However, operational information sharing, involving case-specific or personal data, remains considerably less widespread. The FATF report makes the interesting conclusion that they are constrained mostly by legal and data-protection uncertainty rather than by technical limitations.

While strategic information sharing has become common in jurisdictions, many low-capacity jurisdictions are yet to take advantage of its potential. Strategic information sharing triggers a virtuous cycle that helps foster better risk understanding and risk-based response across an AML/CFT ecosystem. There are some immediate and concrete outcomes of PPPs at a strategic level, which every jurisdiction should tap into.

First, they enable joint construction of typologies, whereby FIUs and obliged entities together document emerging patterns, allowing transaction-monitoring rules to be updated quickly. Second, PPPs provide structured feedback to obliged entities on the quality of regulatory reporting, helping them recalibrate their Suspicious Transaction Report (STR) filings, rather than keep filing low-value STRs. A third advantage is that PPPs facilitate joint training that keeps compliance staff of obliged entities current with the crime threat landscape rather than relying on static typology compilations.

After four rounds of FATF Mutual Evaluations, a significant number of jurisdictions are now largely compliant with FATF's technical standards. Hence, the focus is now entirely on effective implementation of these standards. PPPs are a force multiplier in developing an effective AML/CFT system. No wonder, the priorities of the United Kingdom presidency explicitly commit to enhancing public-private, cross-border, and private-to-private information sharing, consistent with fundamental rights and data-protection safeguards.

Private-to-Private Partnerships

Unlike PPPs, Private-to-private partnerships do not depend on authorities for every exchange. Typically, obliged entities collaborate directly with one another to share risk indicators, counterparty data, and typologies. Subject to data protection laws and no-tipping-off requirements, P2P could even extend to sharing of STRs between obliged entities. While authorities do not intermediate the process, P2Ps also need to be fostered through policy initiatives.

“FATF's 2026 report identifies P2P sharing as the least mature dimension of information-sharing architecture in most jurisdictions.”

The enabling factors required for successfully running P2P partnerships are, inter alia, specific legal provisions, governance structures to manage shared liability, and privacy-enhancing technologies to reconcile data protection obligations with operational-level data exchange.

The distinctive contribution of P2Ps lies in the network effects they generate. Where a single obliged entity can only see part of a transaction happening through its books, a P2P mechanism allows participating

institutions to reconstruct a fuller picture of the transactions. It helps them exchange, for instance, beneficial ownership data, markers of connected mule-account rings, or PEP status.

This effectively removes arbitrage of criminal elements in engaging in complex transactions across financial institutions to fool transaction monitoring. Thus, when P2P information exchange is institutionalised, it raises the baseline defensive posture of the industry as a whole. Financial integrity gets enhanced exponentially rather than linearly.

P2P partnerships are also important, in practice, for detecting sanctions evasion techniques to bypass targeted financial sanctions. The implementation of sanctions screening by FIs and DNFBPs has improved across jurisdictions in the aftermath of the 4th Round of FATF evaluations. However, this only means that actors engaged in terrorism financing and proliferation financing.

FATF's own analysis is explicit that P2P and public-private mechanisms should be viewed strategically together: P2P collaboration is often more effective at prevention, since it operates before a suspicious transaction is even reported, while PPP collaboration remains indispensable for investigating complex networks that require law-enforcement authority and cross-institutional legal process to unwind.

FIU-India's Institutional Architecture: FPAC and ARIFAC

Various competent authorities in India have explored the benefits of PPPs through joint working groups and projects.

“India's FIU has convened a PPP called “FIU-India Initiative for Partnership in AML/CFT” (FPAC), and provided a formal structure to a P2P called the “Alliance of Reporting Entities in India for AML/CFT” (ARIFAC).”

FPAC was launched in January 2022 with the financial sector regulators, 68 obliged entities as permanent invitees, and a further five entities as special invitees. Membership was deliberately calibrated to reflect India's geographical and sectoral spread, its exposure to emerging financial technologies, and the country's distinctive socio-economic landscape.

Over time, it has expanded to include a diversity of financial institutions and designated non-financial businesses & professions. FPAC operates through quarterly plenary meetings supplemented by ad hoc issue-based working groups. The working group discussions bring together the obliged entities, law-enforcement agencies, academic institutions, and technology providers, with the objective of producing thematic risk reports and best-practice guides. The working groups have also been useful in facilitating tactical intelligence sharing.

ARIFAC was designed to work in tandem with FPAC, although it was acknowledged that a P2P forum would take a trajectory of its own. ARIFAC organises collaboration among obliged entities themselves, around four interlinked objectives: structured information and knowledge sharing; the collective development of typology reports, red-flag indicators, and sectoral best-practice papers; capacity building through tiered training and certification programs; and cross-sector collaboration on risks.

One of the first things ARIFAC did was to instigate conversation between compliance officers of different obliged entities across all the sectors. This itself helped increase seriousness in the private sector about financial integrity.

“This networking soon led to collaboration in understanding of new money laundering and fraud risks, such as mule-account networks, sanctions screening gaps, and the abuse of synthetic IDs in the KYC process.”

ARIFAC's certification programs^[1] started more recently but have seen heightened interest from professionals interested in a career in financial crime compliance. The certification program is rigorous and helps build general capacity in the financial crime compliance industry.

Taking on the challenge of wide geographical diversity, ARIFAC convenes thematic meetings regionally as well. However, ARIFAC has not yet ventured into operational information sharing. Typologies and sanitised case studies are frequently shared across ARIFAC networks, but it still lacks an institutional process for routine,

sharing of operational data. A working group at ARIFAC is actively studying data protection laws and technological solutions to deepen understanding of what is possible in operational information exchange.

Outcomes

The outcomes of FIU-India's PPP and P2P initiatives provide preliminary yet instructive evidence of how these initiatives can enhance the effectiveness of AML/CFT systems.

Best-practice exchanges through FPAC and ARIFAC have improved the obliged entities' understanding of the technical formats required for timely STR filing, directly addressing quality gaps in financial intelligence reaching FIU-IND.

The sharing of anonymised case studies and emerging red flags has allowed financial institutions to update transaction-monitoring rules and institutional risk assessments on a more frequent basis. P2P exchanges have helped weaker, less-informed institutions learn from institutions with better compliance, thus denying criminal networks the convenience of migrating to weaker, less-informed institutions.

“Interviews with ARIFAC members have revealed that P2P collaboration has helped in the process of conducting enhanced due diligence, as well as in understanding which customers are low risk, warranting simplified due diligence.”

While operational data on clients are not shared through ARIFAC, compliance officers securely exchange non-public risk indicators on beneficial ownership structures, politically exposed persons, and shell-company networks. This helps develop more targeted procedures for applying a risk-based approach to customer due diligence.

Finally, ARIFAC's tiered training and certification program has begun to standardise AML/CFT professional competence across a historically fragmented obliged-entity ecosystem, extending expertise beyond the chief compliance officer to compliance teams and frontline staff.

[1] <https://arifac.com/>

Conclusion

Digitalisation of the economy has altered financial crimes fundamentally. PPPs and P2Ps represent complementary institutional responses to this shift. While PPPs accelerate capacity and readiness by connecting state intelligence with private-sector operational data, the latter enhances financial integrity across the industry. P2Ps are more potent, in the sense that they help jurisdictions tap into 'network effects' to scale compliance and deepen risk understanding across obliged entities. Yet, P2Ps are less prevalent than PPPs, as evidenced by FATF's 2026 report on PPPs.

As the focus of Mutual Evaluations is shifting towards effectiveness, it is timely to work on national PPP and P2P partnerships and exploit their benefits.

India's FPAC and ARIFAC architecture offers an early but instructive case study of how these principles can be operationalised at scale in a large, sectorally and geographically diverse economy, with gains in financial intelligence quality, typology responsiveness, due diligence, risk-based supervision, and professional capacity.

Smarak Swain

CHALLENGES, CONSIDERATIONS AND BARRIERS TO EFFECTIVE PUBLIC-TO-PRIVATE INFORMATION SHARING



Rachel Waldren | Financial Crime Partner, KordaMentha

“Money laundering is a serious problem, with research indicating organised crime cost Australia between \$35.5 billion and \$82.3 billion in 2023/4.”

Stopping money laundering within Australia and across global borders means everyone needs to work co-operatively, which includes sharing information through public and private partnerships to prevent financial crimes.

While this is an overarching goal, achieving it is not without its challenges in the absence of appropriate legislative frameworks in place to protect privacy and facilitate co-ordination.

The Financial Action Task Force (FATF), the international body that oversees the global architecture to help prevent financial crime encourages its member states, including Australia, which is a founding member, to foster collaboration between organisations working across the public and private sectors. This is so they can share intelligence in a timely fashion and act quickly to prevent crimes, while also respecting data privacy laws.

“Australia is a leader in cultivating co-operation between the public- and private-sector to detect, disrupt and prevent financial crimes and was one of the first countries to set up a formal alliance to connect organisations working across the public and private sectors, the Fintel Alliance.”

The alliance comprises financial institutions, remittance service providers, gambling operators, law enforcement and government agencies who develop shared intelligence and identify ways to detect, disrupt and prevent serious crime in real time.

Industry representatives and law enforcement agencies co-locate within AUSTRAC’s Melbourne and Sydney offices to share and analyse financial intelligence to investigate and disrupt criminal and terrorist activity.

The Fintel Alliance’s work is producing real results, most recently in relation to uncovering coordinated mortgage fraud and systemic weaknesses across Australia’s lending sector. The alliance was able to identify the names of people and entities involved in potentially hundreds of millions of dollars of fraudulent mortgage loans, mostly related to Sydney properties and make referrals to law enforcement partners. It also issued practical controls to lenders to prevent, detect and disrupt mortgage fraud. This is an excellent case study of how public-private partnership can support information sharing within current data privacy laws.

Collaboration can achieve great outcomes, but Australia still has hurdles to overcome to effect FATF recommendations around encouraging information sharing between the private sector and regulators. This is a limitation AUSTRAC acknowledges, recognising inconsistent customer identification, reporting and information-sharing standards limit the ability to track the movement of funds across borders.

These shortcomings are among a number of constraints preventing genuine co-operation outside the Fintel Alliance’s current arrangements, which essentially comprise a ring-fenced environment.

Non-member organisations, typically smaller entities that may be higher risk for money laundering and other serious crimes, may not always have a seat at the table and may not have access to the information they need to identify financial crimes.

Although membership of the alliance has expanded, restrictions on who can take part mean there may be limits on what, and how far, intelligence can be shared. Given the recent reforms to the AML/CTF laws to include lawyers, accountants and real estate agents, consideration needs to be given to how information about intelligence relevant to these sectors can be better shared to help prevent money laundering.

“The question is how to break down barriers to membership of the existing public-private partnership, if that is what is standing in the way of more effective information sharing, and whether a more substantive legislative change to privacy laws is required for broader information sharing.”

Overseas jurisdictions have addressed the challenge of supporting information sharing between smaller private sector entities. In the UK, there has been public-private co-development of a strategic national economic crime plan for fraud and AML that moves towards more widespread data collaboration.

In Australia, consideration should be given to the nature of any mechanism that broadens the Fintel Alliance’s membership, keeping in mind consumer privacy protections.

Considering these options, we shouldn’t be deterred by existing barriers preventing the sharing of information. Rather, we should use existing mechanisms, look to other jurisdictions that are pressing ahead and consider how we leverage public-private partnerships. Now is the time to explore how this can work to stop criminals laundering money through our economy, as well as more serious crimes, and also strengthen the financial system.

In the Netherlands, the Financial Intelligence Unit (FIU) encourages a wide range of national partnerships and work is presently being done on legislation for more AML collaboration.

Back in Australia, 2025 reforms to tipping off provisions offered some flexibility when it comes to information sharing. But there is an opportunity to broaden awareness about how the tipping off provisions work and how they may be used in circumstances that would not, or could not, be reasonably expected to prejudice an investigation.

As overseas examples show, it is possible to widen the net when it comes to giving the right people access to timely information about the potential for financial crimes.

Rachel Waldren

DISRUPTING FINANCIAL CRIME THROUGH PRIVATE-TO-PRIVATE INFORMATION SHARING



Ben Scott | Head of Industry, Government and Relationship Management, Australian Financial Crimes Exchange Ltd | Researcher, Financial Integrity Hub

Financial transactions, both criminal and legitimate, are based on the sharing of information. Individuals and businesses use financial institutions to safeguard wealth and process transactions, and all of this depends on basic, accurate financial information being available at call. Where the transactions are illicit, that financial information takes on an additional value. Now it can be used to stop losses, freeze funds, and commence investigations – but only if it is shared. In the context of financial crime, information-sharing is a fascinating and problematic space, raising a number of questions.

“What information, if any, is appropriate to share and when? With whom can it be shared and for what purpose? What are the respective roles of the government and the private sector in information-sharing?”

This article focuses in particular on the role of information-sharing between private sector organisations to detect, prevent and disrupt financial crime.

It is useful to contrast private sector information-sharing with private-public information sharing built into Australia’s AML/CTF regime. This takes the form of reporting suspicious matters and transactions to the government and Financial Intelligence Unit (FIU) AUSTRAC, for use by law enforcement, revenue, and intelligence agencies. This statutory information-sharing regime was put in place because governments realised that banking institutions held information crucial to detecting and stopping financial crime.

In parallel, there exist less formalised but important private-to-private information sharing channels between financial institutions, particularly where fraud is concerned.

This work is done in a variety of ways, from sharing up-to-date intelligence about fraud methodologies through industry forums, to operational contact between fraud teams to recover funds. In some jurisdictions, industry-developed platforms support these activities. These capabilities do not rest on statutory obligations to report. They are based on organisations’ collective intent to share information for the purpose of fraud and scam prevention, consistent with the terms of their agreements with customers and applicable laws and policies on privacy and information collection.

The information-sharing challenge has become more pressing in recent years, driven by changes in payments technology, consumer behaviour and crime. The financial services industry’s transition to online banking reduced the level of face-to-face interaction required to open an account. In Australia, the introduction of real-time payments in 2018 made payment processing more rapid, with benefits for law-abiding customers, and unfortunately, also for the criminally-inclined.

These trends converged with an explosion in a subset of fraud activity which Australia terms ‘scams,’ where a consumer is induced through deception to authorise a payment direct to a scammer. The harms scams cause to victims are incalculable, and the growth of this technology-enabled ‘volume crime’ in recent years puts existing information-sharing models under strain.

“Financial crime intelligence and investigation resources in government are finite. Fraud investigators do not grow on trees. Too much intelligence is as big a problem as too little; it results in useful signals being drowned in the noise of defensive reporting.”

In this context, the disruption model is useful. It encompasses responses to crime which attack criminal capabilities at their source rather than trying to target every scammer.

Private-to-private information-sharing is a force multiplier for disruption. While financial technology has enabled the rise of scams, it also supports data-led identification and targeting of illicit funds flows, and monitoring high-risk customers. Banks and other reporting entities have sophisticated programs to do just this. If actionable scam intelligence identified by individual entities is then shared across industry, scammers lose their opportunity to act because their network is shut down in near-real time. This is why the sharing of Actionable Scam Intelligence, across industry and with government, is a core obligation under *Australia's Scam Prevention Framework*, which comes into force in March 2027.

So where scams are concerned, government recognises the value of private-private financial intelligence-sharing as an indispensable element of network protection, and has mandated it for that reason.

It is equally important in meeting other financial crime threats. A 2017 Financial Action Task Force (FATF) guidance highlighted the importance of information sharing amongst private sector entities to increase the effectiveness of their AML/CTF efforts. The primary obstacle FATF identified to this kind of information-sharing was the complexity of balancing competing public interests in privacy and crime prevention. In this respect it highlighted the importance of clear regulatory guidance in helping private sector entities negotiate this complexity. In particular, FATF highlighted examples of data protection and privacy authorities working with AML/CTF regulators to provide such guidance, and noted that this was instrumental in providing clear guardrails for private-private sharing initiatives.

FATF also recently published a report on public-private partnerships (PPPs), highlighting the effectiveness of these in combating financial crime. Models for these partnerships include Australia's FIU-led, highly operational Fintel Alliance where law enforcement, banking and AUSTRAC staff work side-by-side. Other models focus more on the sharing of strategic intelligence and typologies. PPPs benefit from clear legal frameworks which give participants confidence to share operationally useful intelligence, rather than reducing the scope of sharing to minimise risk.

Clearly private-private and public-private intelligence sharing each have their place in an effective, holistic response to financial crime. How are they different and what value can each deliver? State and federal governments have limited resources to deal with volume crime. They have intelligence-gathering and enforcement powers which are not available to banks and other private-sector organisations that operate for profit. The financial intelligence capabilities of banks and other businesses extend from their obligations to prevent financial loss and protect their network from being exploited by criminals. Government agencies will always have the lead on investigating serious crime, asset seizure and the targeting of serious criminal groups through enforcement action.

But those actions require intensive efforts and must be targeted to the highest threats. Where criminal threats, such as scam syndicates, target Australian residents anonymously from outside the jurisdiction, it limits the ability of law enforcement to respond.

"In those cases, the priority should be disruption; protecting the financial network by sharing intelligence to stop transactions, block accounts and shut down the ability of these groups to act through the financial system."

Government should see that picture too; industry disruption should not happen at the expense of law enforcement visibility. But it is not necessary, or realistic to deploy broad enforcement powers against every criminal threat. What matters is protecting the customer and the network, and that is where private-private intelligence sharing can spread the load.

Of course for all of this to happen the right regulatory guardrails and guidelines must be in place. That is why FATF endorses clear guidance from government on balancing privacy and intelligence-sharing objectives. Providing that guidance may require collaboration and consensus between privacy and AML/CTF authorities. That will ensure that private sector organisations share what is lawful and appropriate without defaulting to a low-risk de minimis standard. Australia should build on current effective and successful private-private and public-private initiatives to ensure that our information-sharing frameworks protect the financial network against current and emerging threats.

Ben Scott

LESSONS FROM ESTABLISHED INFORMATION SHARING MODELS FOR PUBLIC PRIVATE PARTNERSHIPS IN AUSTRALIA AND INTERNATIONALLY



Dr Paula Chadderton | Government Lawyer and Policy Advisor, Australia

Information sharing initiatives targeting financial crime seek to improve knowledge of criminal networks and typologies, augment strategies to identify transactions linked to financial crime, and posture regulators, law enforcement agencies, the financial sector and communities to take preventative action to inhibit criminal activities. This paper compares initiatives in Australia, Canada, the UK and the US. It considers how information is shared, the benefits and challenges of each model, and the lessons for strengthening public-private collaboration.

Information Sharing Models

Information sharing can occur in several ways:

- linear transfers where information is transferred from one party to another;
- query/response exchanges where information is requested by one party and provided by another;
- broadcast models where a central hub pushes requests for information to multiple organisations for response;
- networked connectivity where one party's information holdings can be accessed directly by another party (subject to controls); and
- centralised connectivity where multiple parties upload information to a shared database that multiple parties can access independently and asynchronously.

Having introduced the primary methods used to share information, this paper now examines how public-private sector information sharing initiatives use them.

Model 1: Australia's Fintel Alliance and UK's Joint Money Laundering Intelligence Taskforce (JMLIT)

Australia's Fintel Alliance (led by the Australian Transaction Reports and Analysis Centre (AUSTRAC)) and the UK's JMLIT are broadly similar public-private

information sharing initiatives that use existing anti-money laundering and counter-terrorism financing (AML/CFT) reporting, and other information sources, to build a multi-dimensional picture of criminal networks. Both initiatives enable members to identify criminal-linked financials and support them in taking preventative or investigative action on financial crime.

"JMLIT is widely regarded as a model for public-private information sharing, while Fintel Alliance is considered distinctive for its co-located public and private sector analysts."

Both initiatives rely on existing AML/CFT reporting obligations, supplemented by other mechanisms, including industry briefings and forums on financial crime trends. Fintel Alliance also uses compulsory production notices to private sector members to collect information pertinent to its activities.

Both JMLIT and Fintel Alliance use a hub-and-spoke approach to manage information. Members upload information an AUSTRAC or JMLIT platform (or portal) (the hub), which is used to disseminate information to all members (the spokes). Recent UK reforms have expanded the circumstances in which private sector sharing can occur, while Fintel Alliance members remain constrained unless disclosure is otherwise authorised by law.

Fintel Alliance and JMLIT's legislative basis also differs. UK legislation specifically underpins JMLIT's information portal. By contrast, while Australian reforms in 2017 and 2019 strengthened AUSTRAC's ability to share information with government agencies, they did not expressly empower Fintel Alliance's portal.

Fintel Alliance's co-location model has a twofold benefit: overcoming legislative barriers that restrict public-private sector information sharing, while facilitating greater understanding of financial crime risks and typologies across sectors. That said, private sector members remain concerned about potential exposure to regulatory non-compliance proceedings arising from their participation or the actions of co-located analysts.

Fintel Alliance has expanded from 18 to 30 members, including government agencies, financial sector entities, a university and two international members. Fintel Alliance's membership has not been without criticism. Its decision not to involve entities now considered relevant to financial crime including insurers, smaller remitters, technology and telecommunications firms, NGOs and newly regulated designated non-financial businesses and professions (DNFBPs). Involving these sectors may provide Fintel Alliance with valuable insights on criminal networks and trends and increase the relevance of its work to a broader audience.

In contrast, JMLIT has grown from 12 to more than 200 partner organisations including government agencies, major banks, investment and insurance firms, technology and telecommunications companies, fintechs, DNFBPs and gaming enterprises. This breadth arguably strengthens JMLIT's ability to target financial crimes and other national security threats facing the UK.

“Together, the Australian and UK models show that collaboration is strongest when supported by clear legal authority, diverse membership and mechanisms that build trust across sectors.”

Model II: Canada: FINTRAC's Project PROTECT and other projects

Canada's AML/CFT information sharing model is more linear, reflecting Canada's strict privacy and human rights constraints. FINTRAC may disclose information if an exception to the prohibition against disclosure applies, or if law enforcement agencies consider there are reasonable grounds to believe that the information is relevant to a money laundering or terrorism investigation. These restrictions significantly impede what information can be shared, when and with whom, causing FINTRAC to be criticised as 'reactive' not proactive.

FINTRAC projects have focussed on single predicate offences as diverse as human trafficking, fentanyl trafficking and romance fraud scams. They rely on suspicious matter reports (SMRs) (or suspicious activity reports) and other AML/CFT reporting that financial institutions identify as relevant to a Project. FINTRAC analyses this information before disseminating it as actionable intelligence to law enforcement agencies.

“While FINTRAC's linear approach may reduce financial institutions' legal and regulatory exposure, law enforcement agencies have criticised its disclosures as tardy, and too generalised, in character.”

Nevertheless, FINTRAC Projects have increased industry awareness of criminal typologies resulting in SMRs containing more actionable intelligence for law enforcement agencies. They have also encouraged financial institutions to refine their financial indicators, and transaction monitoring and reporting systems. The model illustrates the tension between strong legal safeguards, which protect fundamental privacy and human rights principles, and timely public-private sector information sharing, which could bolster efforts to combat financial crimes and the networks and perpetrators involved in them.

Model III: US Section 314(a) Scheme

The US Section 314(a) Scheme uses a broadcast model that takes advantage of the US' enormous financial sector's holdings. Under the Scheme, the US Treasury's Financial Crimes Enforcement Network (FINCEN), acting on behalf of a law enforcement agency, requests 14,000 financial institutions to search their records for information about a target and their financial transactions. Institutions with relevant information must respond within two weeks, which FINCEN disseminates to the requesting law enforcement agency.

US law enforcement agencies consider the Section 314(a) Scheme invaluable in linking disparate information and identifying previously unknown criminal network members and facilitators.

As at 1 September 2026, FINCEN had processed 9,343 requests relating to serious money laundering, terrorism financing and terrorism matters. In 2023, 95% of Section 314(a) requests demonstrably advanced an investigation or prosecution.

Model IV: US Section 314(b) Scheme

FINCEN's Section 314(b) Scheme encourages voluntary private-to-private information sharing about money laundering or terrorism financing. Participating institutions receive protection from liability (or 'safe harbour') for information shared and may collaborate on multi-authored SMRs, enabling them to examine financial crime risks, trends, and typologies across institutional boundaries.

Participation in the Section 314(b) Scheme remains more limited than the Section 314(a) Scheme. Reported barriers include the annual reapplication process, uncertainty about what can be shared, and concerns about regulatory or litigation exposure. Notwithstanding its safe harbour protections, the reduced participation in the Scheme is arguably influenced by questions over its clarity, confidence and perceived value.

The US remains one of the few jurisdictions with an express legal basis for private-to-private information sharing, although the UK is considering reforms to support such sharing, and Canada introduced guidance in 2025 for a FINTRAC-led private-to-private sector information sharing initiative.

Lessons Learnt

The initiatives examined suggest that increased, targeted public-private sector information sharing can benefit governments, law enforcement and the community by improving detection of financial crime, increasing awareness of criminal methods and typologies and supporting prevention. The initiatives discussed also offer several lessons for future public-private sector information sharing initiatives.

First, a clear legal basis is crucial. Existing AML/CFT reporting obligations provided the foundation for most initiatives, complemented by other industry or government-specific mechanisms. However, each initiative's governing legislation ultimately determined the extent that information could be shared. Models without clear authority risk being narrow, slow or dependent on workarounds.

Second, safeguards shape participation. Privacy, human rights and secrecy protections are undoubtedly essential, but uncertainty about liability or regulatory exposure, or roles and responsibilities, can deter private sector involvement. While safe harbour protections can

assuage concerns, the US experience shows that protection alone is insufficient if participation is administratively burdensome or operational benefits are unclear.

Third, membership breadth affects effectiveness. Financial crime increasingly cuts across banking, remittance, gaming, fintech, telecommunications, technology, insurance and professional services. Initiatives that do not include relevant sectors, if only temporarily, may overlook opportunities to refine indicators, understand evolving typologies and generate new perspectives.

Fourth, forums, briefings and typology reports can assist to share findings, explain risks, generate discussion on financial crime methods and trends, and thus build trust and confidence between sectors. Moreover, they also offer opportunities to provide feedback on regulatory challenges faced as well as involve organisations that are not formal members of an information sharing initiative and garner their insights.

However, while these benefits are laudable, they also raise questions about the long-term sustainability of public-private sector information sharing initiatives. Initiatives must thus demonstrate operational value.

“Participants, whether from the public or private sector, are more likely to remain engaged where collaboration produces actionable intelligence, supports compliance, advances investigations and mitigates, if not ultimately, prevents harm.”

Co-location may be considered the 'gold standard' in facilitating collaboration, but it is resource intensive and may not be sustainable without clear benefits.

The models examined highlighted how expanded public-private sector collaboration can strengthen responses to financial crime. However, their success ultimately depend on the existence of a clear legal basis, appropriate safeguards, trusted and diverse participants, and ongoing evidence that public-private sector collaboration produces practical results that prevent financial crimes.

Disclaimer: The views expressed in this article are the author's own and do not reflect those of the Australian government.

Paula Chadderton

FROM SOCIAL NETWORKS TO FINANCIAL NETWORKS: THE EMERGING TERRORIST FINANCING CHALLENGE AND WHY COLLABORATION IS THE KEY DEFENCE



Nadine Jones | Joint Threat Financing Group, Australian Federal Police

The next evolution of terrorist financing is not a future challenge; it is already emerging within the digital ecosystems used by billions of people every day. Recent work by the Financial Action Task Force (FATF) with the project dedicated to better understanding ‘*Terrorism Financing through Social and Media and Streaming Platform*’ [1] (TF-SMSP), highlights a growing number of case studies and typologies that demonstrate how terrorist actors are adapting to platform-based financial environments, often faster than regulatory and operational responses can evolve.

As social media, messaging and streaming platforms increasingly integrate payments, monetisation tools and virtual assets, they are becoming financial ecosystems in their own right.

“The challenge for governments is no longer determining whether this threat will materialise, but ensuring that partnerships, capabilities and frameworks are developed now so we are not continually responding after new methodologies become established.”

A critical distinction for practitioners is that platforms are exploited for both terrorism purposes and terrorist financing purposes, but in very different ways. Terrorism-related activity typically involves propaganda, recruitment and operational coordination.

Terrorist financing, however, focuses on raising, moving and concealing funds. Increasingly, terrorists are leveraging crowdfunding campaigns, micro-donations, virtual assets, creator monetisation tools and integrated payment functions to generate and transfer value across borders. Detecting this activity requires more than monitoring content; it demands the ability to link online behaviour, financial transactions and digital networks.

The typologies FATF has identified read less like a traditional financial crime taxonomy and more like a map of the modern creator economy turned to darker purposes. Humanitarian-fronted crowdfunding and fake charities solicit small, trust-based donations from diaspora communities, often shifting from public appeals on mainstream platforms to encrypted channels once payment details need to be exchanged. Funds raised are frequently converted through hawala networks, prepaid cards or mobile money to obscure the trail before they ever touch a regulated institution.

Elsewhere, the abuse tracks the platforms' own monetisation tools directly: livestreaming, subscriptions, tipping and pooled donations, the same features that let a legitimate creator build an audience, are being used to generate and move funds under the cover of ordinary engagement. In-app virtual asset wallets, rotating QR codes and dual custodial/self-custodial wallet structures add a further layer of anonymity, while coded language, emojis and community-specific references let requests for money hide in plain sight, framed as humanitarian or religious appeals. Notably, less than a third of jurisdictions contributing to the report currently capture SMSP-related TF risk in their national risk assessments at all, even as those in conflict-affected areas rate the risk as high or very high.

[1]<https://www.fatf-gafi.org/en/publications/Methodsandtrends/detecting-and-disrupting-tf-through-smmps.html>

An emerging challenge goes beyond the direct misuse of fundraising tools and raises broader questions about the creator economy itself. Increasingly, platforms reward creators through advertising revenue, engagement-based incentive schemes, subscriptions, virtual gifts and creator funds designed to encourage audience growth and content production. While these business models are central to the digital economy, they also create the possibility that platforms could inadvertently channel financial benefits to individuals who are cultivating extremist audiences through content that remains below traditional moderation thresholds.

Unlike overt terrorist fundraising campaigns, these creators may never explicitly ask for donations or openly advocate support for a terrorist organisation.

“Instead, they may rely on coded language, dog whistles, conspiracy narratives, historical revisionism or grievance-based messaging that subtly promotes extremist ideologies while avoiding content enforcement mechanisms.”

Where monetisation eligibility is determined primarily by engagement metrics, views, watch time or audience interaction, financial rewards can be generated directly from platform activity rather than from deliberate donations by supporters.

This presents a new and potentially complex terrorist financing question. If content itself becomes a revenue-generating asset, and that content serves to normalise, promote or cultivate extremist ecosystems, at what point does platform-generated income become an indirect financing pathway? FATF has already identified the exploitation of creator-economy monetisation features as an emerging typology, noting that engagement-based earnings, pooled donations and other creator monetisation mechanisms can blur the line between legitimate revenue streams and funds connected to extremist ecosystems.

For policymakers, regulators and industry, this challenge sits at the intersection of content moderation and financial crime. Traditional AML/CFT frameworks

focus on tracing suspicious financial transactions, while trust and safety frameworks focus on harmful content. The next frontier may require understanding how influence, engagement and monetisation interact to create new financial pathways that do not fit neatly into either model.

As platforms increasingly monetise attention and reward audience growth, understanding whether monetisation systems can inadvertently support extremist actors will become an important area for future risk assessment and public-private collaboration.

Part of the challenge is structural. Social media and streaming platforms do not generally fall within sectors directly subject to AML/CFT obligations under the FATF Standards. Yet many now facilitate financial activity through in-app payments, virtual asset wallets, tipping functions, creator payouts, social commerce and embedded payment services. As financial functionality becomes increasingly integrated into platform ecosystems, traditional distinctions between technology companies and financial service providers are becoming blurred. The question is no longer whether a platform is a social media company or a financial institution, but what financial activities it enables and how those activities should be managed from an AML/CFT perspective. The implications are significant.

“Digital platforms offer terrorist actors global reach, rapid information exchange, anonymity-enhancing features and access to vast user communities. These same characteristics also place the challenge beyond the reach of any single agency, regulator or jurisdiction.

No organisation holds the complete picture.”

Technology platforms can observe behavioural indicators, financial institutions can identify suspicious financial activity, and governments can contribute intelligence, investigative powers and threat context. Individually these insights are limited; together they become actionable intelligence.

“This is why public-private partnerships must become a cornerstone of future counter-terrorism financing efforts.”

FATF's work reinforces that stronger collaboration between social media platforms, financial institutions, virtual asset service providers and government agencies is essential to understanding and disrupting emerging terrorist financing methodologies. Platforms possess data, technological capabilities and early warning signals that law enforcement often cannot access independently.

Conversely, authorities can provide the contextual intelligence needed to distinguish suspicious activity from legitimate platform use. Effective information-sharing arrangements bridge this gap and enable earlier intervention.

Australia has already demonstrated the value of a proactive approach through initiatives that bring government, regulators and industry together to address online harms. The challenge now is ensuring this same forward-leaning posture extends into the financial dimension of digital platforms. The financialisation of social media is accelerating, and terrorist actors will continue to adapt to new opportunities.

The challenge ahead is not simply identifying fundraising campaigns hidden on digital platforms; it is understanding whether the economic architecture of the modern creator economy can itself be exploited to generate and sustain extremist ecosystems. Meeting that challenge will require governments, financial institutions and technology companies to work together before these risks become embedded features of the digital landscape.

Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the views, positions or policies of the Australian Federal Police (AFP).

Nadine Jones

INTEGRATING THE PURPOSE LIMITATION AND FISHING EXPEDITION PROHIBITION PRINCIPLES IN THE IMPLEMENTATION OF PUBLIC-PRIVATE PARTNERSHIPS



Dr Go Lisanawati | Professor, Faculty of Law, University of Surabaya, Indonesia

Public-Private Partnerships play a crucial role in the anti-money laundering and counter-terrorism financing (AML/CFT) regime. However, it is undeniably facing challenges. One such challenge is protecting customers' personal data. Potential violations include breaches of the 'Purpose Limitation Principle' and 'Prohibition of Fishing Expeditions Principle'. There is a very high likelihood of a conflict arising between the obligation to share financial intelligence for the sake of national security and the obligation to share data without the customer's consent.

“Collaboration between the public sector and the private sector could face a critical dilemma between regulation and operational implementation.”

Risk of Breaching the Purpose Limitation Principle

Essentially, purpose limitation is a data protection rule that requires organisations collecting personal data for specific, legitimate, and clear purposes to disclose those purposes to the data subject from the outset. It is not allowed to process the data beyond those purposes. That data should be collected only for legitimate and specific purposes. Meanwhile, under AML/CFT regulations, exceptions to data confidentiality are necessary. The processing must be consistent with the purposes specified from the outset and must not be used for other purposes without notifying the data subject or obtaining their consent. The processing purpose and the data use must be clear and communicated to the data subject. Using data that is not aligned with its original purposes requires providing the data subject with adequate information about its use, and obtaining further consent.

In this context, personal data should be collected for specific, explicit, and legitimate purposes; processed only in accordance with the original purposes; and must not be used for other purposes incompatible with the original purpose, unless there is a valid legal basis.

Does the disclosure of data for the prevention of money laundering also violate the principle of purpose limitation? In the context of AML/CFT, this principle could be considered as a legitimate exception required by a greater interest, rather than a violation. AML/CFT regulations impose a legal obligation on reporting Entities to process and monitor data. This obligation is not contingent on customer consent but based on statutory requirements. In this sense, the restriction provides an exception grounded in the public interest and law enforcement. In data protection law, data must be used with a clear purpose and on a legal basis.

What must be prevented is that, even in the interests of the legal principles mentioned above, it is still not permissible to cause harm to the public, resulting in sporadic account freezes, or even undermining trust in the legal profession itself.

There is a clear potential for a conflict of interest between the protection of personal data and the public interest in combating money laundering. So, how should the law resolve this conflict? Essentially, it needs to look to the proportionality principles and apply them. Restrictions on data protection are permitted if certain conditions are met, including: the existence of a legal basis, in this context, the obligation to report suspicious transactions under anti-money laundering principles, while disclosure without such a legal basis constitutes a violation. The disclosure must be proportionate to the purposes, even without the customer's consent.

Prohibition of Fishing Expedition Principles: Is it a Must?

The ‘Fishing Expedition Prohibition Principle’ prohibits authorised parties from searching, collecting, or disclosing information extensively without a clear basis, reasonable grounds, or a specific purpose. Criminal procedural law, personal data protection, privacy rights and intergovernmental information exchange develop this principle widely. In simple terms, fishing expeditions are attempts to search for evidence or information in a random, widespread, and speculative manner in the hope of finding a violation of the law, without any basis for suspicion or clear purpose.

In the view of AML prevention, this principle is important because the AML regime gives broad authority to institutions such as Financial Intelligence Units (FIUs), law enforcement officials, and financial institutions to access and analyse financial data. The authority must not be unlimited. Without this principle, the authority of the AML/CFT institutions can develop into huge and unlimited activity that could risk causing a function creep. They may supervise all community financial activities, mass profiling, social surveillance, and the purposes for which data are used. The more data the state has, the greater the risk of misuse.

Meanwhile, the AML/CFT regime absolutely needs to increase public trust. In this capacity, a state (authority) needs to certify that the system must not allow data to be accessed without a reason. Once access is granted, it should be followed by a legal basis. The legitimacy of voluntary compliance depends on institutional trust.

The AML/CFT regime needs to limit access through several principles based on necessity, proportionality, legality, accountability, purpose limitation, and prohibition of fishing expeditions. However, as an authoritative agency, it still cannot request all public data without a reason that can be accounted for.

Constructing Reasonable Suspicion as a Balance Model Protection for Data and Privacy

In the AML/CFT regime, indicators of Suspicious Transaction Reports (STR) and Suspicious Activity Reports (SAR) are important, but they should not be equated with reasonable suspicion. STR/SAR is an operational manifestation of the existence of reasonable

suspicion, while reasonable suspicion is a legal standard that is the basis for justifying state actions. Reasonable suspicion gives the obligation to prepare an STR/SAR and provides a legitimate basis for the FIU or officials to access further data within the limits of their authority. STR is a documented indicator that the reporting party has met the reasonable suspicion standards. STR is not automatically considered to meet reasonable suspicion. The quality of protection of personal rights does not depend on the quality of compliance of the institutions that are the subject of the reporting entry (in this regard, the private sector).

“Meanwhile, the restriction of the right to privacy must meet the requirements of legitimate, necessity, and proportionality principles as a guarantee of reasonable suspicion itself.”

Thus, reasonable suspicion in the AML/CTF regime must be built as a multi-factor legal standard that requires more effort and reasons to exercise its functions. It can start from the existence of suspicious transaction indicators as an initial indicator. It also needs contextual evidence, as in CDD/EDD, a risk-based approach based on customer profiling, and analytical linkage as a limitation on fishing expedition violations.

The STR/SAR is not positioned as an automatic permission to access wider data, but rather as an initial indicator that must pass a series of legal tests before generating a legitimate reasonable suspicion. This approach not only strengthens the protection of personal data, but also improves the quality of financial intelligence analysis because any data access is based on objective, documented and auditable reasons.

Hence, the legitimate purpose of AML/CFT does not automatically mean providing the authority to conduct indiscriminate data searches. The collection, access, aggregation, and analysis of data must still have a predetermined purpose, be relevant to that purpose, and be proportionate. Public-Private Partnerships must be speculative, excessive, and should have limits on authority in data processing.

Go Lisanawati

NEITHER SHARING NOR PROTECTION: WHY DATA PROTECTION LAW MISSES AML DATA PROCESSING



Umay Şener | Lawyer | PhD Researcher, Cardiff University School of Law & Politics, UK

The Financial Action Task Force (FATF) Recommendations require states to designate some private entities as obliged entities and make them do something no commercial relationship would ask: collect data for the state to help prevent and detect crimes.

“Preventive measures have largely been devolved to the private sector, casting these firms as sentinels guarding the legal economy against illicit finance. They are not investigators, but the work is investigative and the purpose is the state's.”

Which law governs the personal data processed for this purpose? For the Financial Intelligence Units (FIUs), this has been actively disputed. For obliged entities, no such argument took place. Data protection law's applicability was assumed, and the debate moved straight to its application.

The relationship between Anti-Money Laundering (AML) obligations and data protection law is conventionally described as a balance: effectiveness on one side, privacy on the other. Balance implies a common purpose. AML and data protection have none. Forcing one onto the other misses both protection and effectiveness. For example, voluntary private-to-private sharing goes largely unused; the accuracy of Suspicious Activity Reports (SARs) goes unchecked. Data protection law was drawn around a custodian: an institution that decides for itself what to collect and answers for it to the person it collected from. Obligated entities do neither in full. They collect because the state requires it, and the account they give is owed to the state. The wrong instrument is being applied, and it leaves individuals unprotected and enforcement ineffective.

Where Neither Regime Reaches

Data protection laws are typically prohibitive by default: processing is prohibited unless a listed ground applies. The institution cannot reach the question of whether sharing would be harmful or useful until a ground is available to it. Where AML processing is mandated, the legal obligation supplies the ground and the question answers itself. Voluntary private-to-private sharing between unrelated institutions has no such foundation in the Recommendations.

“Although FATF treats this as critical to detecting money laundering, and accepts that a single institution cannot see enough to identify complex schemes on its own, it requires no sharing beyond correspondent banking, wire transfers, third-party reliance and group-wide programs the last of which runs within a corporate group, not between the unrelated entities the problem concerns.”

National law can supply what the standards do not. The United Kingdom built voluntary statutory gateways with liability protection attached; on the government's own assessment they enable sharing in principle but are underused or inconsistently applied in practice. The gateway lifts the AML barrier without settling the data protection position, and firms decline to use it because the exposure that remains is theirs to carry.

The Netherlands attempt is an example where the private entities took the initiative and the state followed. Five banks established Transactie Monitoring Nederland (TMNL) to monitor payment transactions collectively, the government's consultation on a bill came afterwards.

The Council of State found the measure a far-reaching infringement of fundamental rights questioned whether the end justified the means, and advised against submitting the bill unless amended. The government amended it, but the sharing provisions were later dropped as the AMLR was set to supersede them. TMNL announced in July 2024 that it would wind down its existing activities and capabilities, because of the upcoming AMLR. However, lawfulness of several years of processing was never assessed. In neither jurisdiction, the data protection position was resolved by anyone with authority to resolve it. The UK settled the AML question and left the rest to the institution; the Netherlands failed to settle the lawfulness question.

Accuracy is the requirement both regimes share. Data protection law makes it a core principle; AML requires customer identity to be verified against independent sources. Yet neither checks it in respect of SARs. In the data protection model, accuracy is enforced principally through the data subject: rectification presupposes access, and access presupposes knowing there is something to see. The crime-prevention exemptions, reinforced by the tipping-off prohibition, remove the data subject's recourse and with it the trigger for regulatory attention. A data protection authority that acts on complaint receives none, and the reports themselves sit behind confidentiality rules that sharply limit what a data protection authority may see. Accuracy can therefore only be checked elsewhere. In AML, that means the supervisory authorities, whose oversight runs through periodic examination of the institution. Examiners may read individual reports during audits, but they read them to evaluate whether the institution's identification, evaluation and reporting process is working. The report is evidence about the system, not the object of scrutiny.

“No part of that review asks whether a particular report was based on correct data. Nor does the FIU close the loop.”

Even where it detects an error, its feedback to obliged entities is directed, by the standard's own terms, at assisting institutions in detecting and reporting suspicious transactions. The object is future performance. An institution that transmits faulty data receives no signal or faces no consequence, and keeps the record that produced it.

The Custodial Assumption

The two failures look unrelated, but both follow from the same mistake: data protection law was built for institutions that choose what to collect, not for institutions required to. Most national data protection laws are not independent inventions. They share common core principles, including collection limitation, purpose specification, use limitation, data quality and individual participation.

In the instruments that shaped them, collection appears only in the language of restraint. The model assumes the institution decides for itself what to collect and why. It does not contemplate an institution collecting because someone else has told it to. An institution may use data for new purposes where the law authorises it, but no equivalent clause widens collection. Therefore, the model cannot imagine a law that orders the institution to actively investigate.

Collection is constrained, never required. The data controllers' duties attached to data it holds and how it handles them. These are custodial obligations, not investigative ones. AML inverts the assumption. The obliged entities do not simply govern what it receives; it is required to seek more.

“Collection is not an event at on-boarding that then attracts safeguards; it is a standing duty for ongoing monitoring. Whether the law prescribes what to gather or leaves it to their own risk judgment, the reason for gathering it is not theirs, and the account they give is owed to the state.”

The fit fails not because the data protection safeguards are too strict, but because their logic is custodial not investigative. The mismatch deepens because much of the relevant data: risk scores, behavioural baselines, network inferences, is generated by the institution.

Inferred data has long been data protection law's weakest terrain: rectification bites on facts, and does little against assessments that are probabilistic by nature. The category of data AML produces most of is the category the general law governs least well.

What Follows?

Legal systems already accept that intelligence work needs rules of its own. Bodies exercising policing functions generally allow individual rights to be exercised indirectly, through a supervisory authority, where direct exercise would prejudice an investigation. But that regime does not reach obliged entities, on two counts. It is scoped by who processes rather than why, and a private institution fails on the who.

It also curtails rights on a premise that does not hold here: the suspicion behind the processing has been formed under legal standards and remains subject to discipline, whereas the obliged entity's suspicion can be generated defensively and more subjectively.

“That leaves the general regime, which fails because it cannot accommodate an investigative purpose. AML obligations are drafted in open terms by design: the law requires risk to be assessed but not on which terms, and reports to carry the necessary information but does not say which data is necessary.”

AML's purpose is to detect what has not yet been identified, so the data required depends on what the existing data reveals. Under data protection necessity, proportionality and minimisation are measured against the data the purpose requires and AML cannot state that in advance. It would be tempting to treat this as an AML drafting problem, curable by tighter definitions. But the openness is not a defect to be corrected; it is what allows the rules to keep pace with criminal methods that adapt to whatever is specified. The question is therefore not how to close the AML rules, but what disciplines the processing given that they remain open. That question belongs to data protection law, and it is the one nobody is positioned to answer.

Private AML processing therefore falls between the general model and the intelligence one: too investigative for a regime that assumes the institution chose its own purpose, too undisciplined for one that curtails rights on the strength of a tested suspicion. What is required is not further exemptions from a template built for another purpose, but a data protection regime written for obliged entities: one that supplies a basis for the sharing the system needs, and vests in a supervisor the power to audit accuracy without waiting for a complaint and to assert on individuals' behalf the rights they cannot assert themselves. Such a regime would not lower the standard applied to obliged entities. It would be the first standard addressed to what they actually do.

Umay Şener

FOLLOW THE DATA, FOLLOW THE MONEY: STRENGTHENING THE LINK BETWEEN CYBER INCIDENT REPORTING AND FINANCIAL CRIME INTELLIGENCE



Ha Do | PhD Researcher, Macquarie Law School, Macquarie University | Lecturer, People's Security Academy, Vietnam

Different Reports, One Criminal Event

Australia's emerging reporting architecture illustrates both the opportunity and the problem. A ransomware incident may generate information through several channels. Under the Cyber Security Act 2024 (Cth), a reporting business entity that makes a ransomware or cyber-extortion payment must report prescribed information within 72 hours. A financial institution involved in processing the payment may separately identify suspicious financial activity and, where the statutory threshold is met, submit a Suspicious Matter Report (SMR) to AUSTRAC. The victim may also report the underlying cybercrime through ReportCyber. Although these reports may overlap, they are not merely duplicative: each captures a different aspect of the same event.

A cyber report may reveal the compromised account, communications with an extorter, malicious infrastructure or cryptocurrency wallet used in the incident. A financial institution may instead see the beneficiary account, customer information and where the funds move next.

“Individually, each fragment provides only partial visibility. Taken together, they may provide a clearer picture of how the crime occurred and where the funds are moving.”

But that picture is only useful if it emerges in time to support intervention. If those connections emerge only after funds have passed through multiple accounts, wallets or jurisdictions, the problem becomes one of investigation and asset recovery.

If relevant indicators can be identified, matched and routed while the funds remain within reach, financial institutions and relevant authorities may have opportunities to intervene earlier. The value of information sharing lies not only in producing a fuller intelligence picture, but in producing it soon enough to change the outcome.

Critically, cyber incident reporting should be treated not as the end of a compliance process, but as the potential beginning of an intelligence chain: report, match, enrich, route, disrupt and feed back. The regulatory challenge is to shorten that chain without sacrificing privacy, confidentiality, cyber security or the trust necessary for candid reporting. It is therefore a regulatory challenge to shorten that chain without sacrificing privacy, confidentiality, cyber security, or the trust necessary for organisations to report candidly.

Cyber incident reporting requires organisations to notify public authorities of qualifying cyber incidents, but the purpose and content of those reports vary across regulatory regimes. In Australia, critical-infrastructure incidents may require notification within 12 or 72 hours; Australian Prudential Regulation Authority-regulated entities may face a separate 72-hour requirement; eligible data breaches engage the Notifiable Data Breaches scheme; and covered ransomware or cyber extortion payments must generally be reported within 72 hours.

These regimes are not interchangeable: they respectively support operational response, prudential supervision, protection from privacy harm, or understanding of cyber extortion threats and payments.

Comparative approaches demonstrate that incident reporting is increasingly being designed not only to collect information, but also to facilitate its analysis, circulation and operational use. The European Union's Network and Information Systems Directive (NIS2) uses staged 24-hour and 72-hour notifications, while the Digital Operational Resilience Act (DORA) applies tailored requirements to financial entities. In the United States, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCA) provides for 72-hour covered-incident and 24-hour ransomware payment reporting once implemented through CISA's final rule; it also contemplates inter-agency sharing, analysis and dissemination.

Under the United Kingdom's current Network and Information Systems regime, qualifying incidents are generally reportable within 72 hours, while a Bill before Parliament would introduce an initial 24-hour notification followed by a fuller report within 72 hours. These regimes illustrate a common challenge: more reporting may improve visibility, but does not automatically produce better intelligence. Where information about the same event enters different regulatory systems, its value depends on mechanisms that can connect, analyse and act on it.

Financial intelligence emerges when reports and indicators are analysed to identify patterns, entities or networks, becoming actionable when sufficiently reliable and timely to support intervention. In Australia, AUSTRAC performs this function using SMRs and other information.

“Cyber and financial reporting may reveal different parts of the same crime: a cyber report may identify a compromised account, malicious domain or cryptocurrency wallet, while a bank may see the receiving account and subsequent movement of funds.”

Connecting these fragments can therefore provide intelligence neither source produces alone. This connection already exists: the US Financial Crimes Enforcement Network (FinCEN) encourages cyber-related indicators to be included in Suspicious Activity Reports, while Australia's Fintel Alliance combines public- and private-sector information to produce

actionable financial intelligence. The challenge is to make it more systematic, timely and legally clear.

Designing the Bridge

A better approach is to connect existing reporting systems in stages, rather than create a single government database containing all cyber, customer and transaction data. Reporting regimes could use a limited set of interoperable indicators, such as beneficiary accounts, wallet addresses, transaction hashes, domains and timestamps, to enable lawful matching across reporting systems.

Under a “match first, disclose second” model, an authorised system would establish whether the same indicator appears elsewhere without exposing the underlying files. Privacy preserving techniques could minimise raw data circulation. A match would remain an intelligence lead, not evidence of crime; fuller disclosure would occur only after human review and satisfaction of a legal threshold.

“Legislation must define what may be shared, by whom, for which purposes, at what threshold, and subject to what access, retention and oversight controls.”

Australia's revised tipping-off offence focuses on disclosures that would or could reasonably be expected to prejudice an investigation, but does not override privacy, secrecy or confidentiality requirements. The distinction between protecting a report and permitting the use of underlying facts is reflected in *Colonial Mutual Life Assurance Society Ltd v Donnelly* [1998] FCA 364. Decided under predecessor legislation, the Full Federal Court held that direct evidence was not rendered inadmissible merely because it recounted events also recorded in a protected report; protecting an SMR therefore need not make every underlying fact unusable.

However, sharing those facts still requires an appropriate legal basis. The s 123(5) exception for prescribed information-sharing arrangements is not yet in operation because the required regulations have not been made. Without clear gateways, some organisations may disclose too much while others remain overly cautious.

Protect Reporting While Enabling Action

Information-sharing powers must be paired with protections that sustain candid and timely reporting. The *Cyber Security Act 2024* (Cth) restricts the use and secondary disclosure of ransomware-payment reports and limits their admissibility against the reporting business entity. These protections do not cover information independently obtained by an authority, preserving enforcement options without turning the report into a source of general regulatory exposure. Once a connection is validated, the intelligence should reach the actor best placed to respond, a bank able to trace or recall funds, a virtual asset service provider able to follow a wallet, a cyber agency able to warn others, or law enforcement able to investigate the network.

“Success should be measured not by data volume, but by whether the right information reaches the right actor while it remains useful.”

Close the Intelligence Loop

Feedback should convert reporting from one-way compliance into system learning. Authorities may be unable to disclose information that could prejudice an investigation, but they can return sanitised indicators, typologies and risk alerts. The NIS2 Directive requires the relevant authority or incident-response team, where possible, to respond to an early warning within 24 hours with initial feedback and, on request, mitigation guidance; Fintel Alliance similarly shows how public and private expertise can produce useful intelligence.

The process should therefore follow this sequence: report → match → enrich → route → disrupt → feed back. It converts visibility into action and learning. Cyber criminals do not separate intrusion, deception and money movement; regulation should not treat them as unrelated merely because information enters through different channels. The aim is not to centralise all data, but to connect the right fragments lawfully, securely and in time to reduce harm.

Ha Do

WHEN INFORMATION MOVES, BUT ACCOUNTABILITY DOESN'T

CASE STUDY: A TANZANIAN PRACTITIONER'S PERSPECTIVE ON PUBLIC-TO-PRIVATE INFORMATION SHARING



Adam Kheri Famao | Governance, Risk & Strategic Advisory Professional Dar es Salaam, Tanzania

Information sharing has become one of the defining pillars of modern financial crime prevention. Financial institutions collect customer information. Regulators receive complaints and supervisory intelligence. Law enforcement agencies gather investigative information. Reporting entities submit information to public authorities. Each actor possesses a piece of the wider picture. But there is a question that deserves greater attention:

“What happens when information moves through the system, but accountability does not move with it?”

My experience with a real-world financial consumer and regulatory matters in Tanzania brought this question into sharp focus. The matter remains subject to ongoing legal processes, so this article does not seek to determine the merits of the dispute or make findings against any particular institution. Instead, I use my experience as a practitioner case study to examine a broader issue: whether information shared between private institutions and public authorities is ultimately converted into effective action, remediation and institutional learning.

When a Customer Complaint Becomes Intelligence

The case study begins with concerns surrounding the opening and operation of a corporate bank account, including questions relating to authorisation, customer identification, Know Your Customer (KYC) processes and subsequent transactions. At first sight, this may appear to be an ordinary customer dispute. From a financial crime and governance perspective, however, such an event can contain much broader intelligence.

- Who initiated the banking relationship?
- Who was authorised to act?
- What KYC information was obtained?
- When was verification completed?
- What controls were operating at the relevant time?
- What happened after the account became operational?
- Were subsequent transactions consistent with the customer information available?
- When concerns emerged, what internal escalation occurred?
- And, when the matter reached the regulator, what happened to the information?

These are not simply questions for resolving a dispute. They are questions about the effectiveness of the control environment. A customer complaint can therefore be much more than a request for redress. Properly assessed, it can become an early-warning signal for weaknesses in customer due diligence, authorisation controls, transaction monitoring, record management or governance. The challenge is ensuring that the signal is not lost after the immediate issue has been processed.

KYC Should Create Institutional Memory

KYC is sometimes treated as an onboarding exercise: collect identification documents, verify the customer and open the account. That is necessary, but it is not sufficient. Effective KYC should create institutional memory. Information obtained at onboarding should remain connected to subsequent customer activity, reviews, alerts, complaints, investigations and regulatory engagement. When a material concern emerges, the institution should be able to reconstruct the customer's journey.

The same principle should apply to the supervisory ecosystem. A regulatory complaint should not exist merely as an isolated file. It can represent valuable supervisory intelligence capable of identifying recurring weaknesses, emerging risks and opportunities for preventive intervention.

“This is where public-to-private and private-to-public information sharing becomes more than the movement of data. It becomes a chain of accountability. The regulator should not be the final destination.”

My experience raised another question that I believe deserves wider discussion. When a regulator identifies a problem or reaches a determination, what happens next?

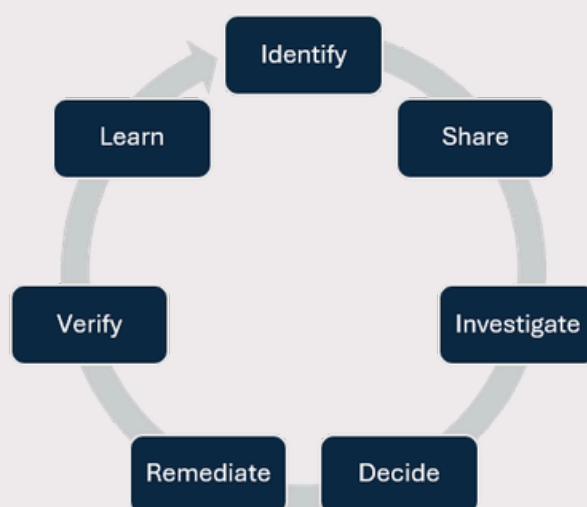
- Is the information simply communicated?
- Is the required action implemented?
- Is remediation documented?
- Is the affected consumer informed?
- Is the underlying control weakness corrected?
- Is implementation independently verified?
- And, is the lesson fed back into future supervisory practice?

A regulatory finding should not be the final destination of information. It should become a starting point for remediation and learning. Otherwise, a system can create an accountability gap in which the customer, financial institution and regulator each possess part of the information, while no single process ensures visibility across the entire journey from identification to remediation.

The Missing Ingredient: The Feedback Loop

A mature financial ecosystem should operate as a feedback loop: A customer complaint may reveal a control weakness. A control weakness may reveal a governance issue. A governance issue may generate supervisory intelligence. Supervisory intelligence may trigger remediation. Remediation should produce evidence; and that evidence should inform future institutional and supervisory practice.

The model should therefore be:



The alternative is, receive, process, close. One model treats information as something to be processed. The other treats information as something from which the system must learn. For financial crime prevention, that distinction matters enormously.

Time

Information does not exist outside time. A regulatory concern that remains unresolved for an extended period can acquire additional consequences. Businesses continue operating, commercial relationships evolve, records can become more difficult to reconstruct, financial consequences may accumulate, and most importantly, confidence in the financial system can deteriorate.

Information-sharing frameworks therefore need more than channels. They need time-bound accountability.

- Who received the information?
- When?
- What action was required?
- Who owns that action?
- What is the expected timeframe?
- What evidence demonstrates completion?
- Who verifies remediation?

These questions should be capable of being answered without reconstructing an entire institutional history from scattered correspondence. Time-bound accountability is therefore not merely an administrative requirement. It is a risk-control mechanism.

From Information Sharing to Information Governance

The broader lesson from this experience is that public-to-private information sharing should not be evaluated simply by asking whether communication channels, reporting obligations, committees, or technological platforms exist. The more important question, however, is whether the information actually produces an outcome: does it reach the right decision-maker, trigger proportionate action, and allow that action to be traced? Can remediation be demonstrated, and does the affected stakeholder understand what has happened? Ultimately, does the system learn from the event and use that learning to strengthen future responses?

These questions move the conversation from information sharing to information governance. That shift is relevant not only to anti-money laundering and counter-terrorism financing (AML/CFT), but also to financial consumer protection, fraud prevention, prudential supervision and broader institutional accountability.

The Uncomfortable Question for Financial Institutions and Regulators

The financial sector increasingly operates on the assumption that better information produces better decisions. That is true, but only when institutions are capable of converting information into action. A sophisticated KYC framework cannot compensate for ineffective escalation, and a strong reporting framework cannot compensate for weak follow-through. Likewise, a regulatory determination cannot achieve its full preventive value if remediation is not measurable. Importantly, a customer complaint cannot strengthen the financial system if it disappears once the immediate dispute has been processed. The objective should therefore be to build systems in which information carries responsibility.

When information moves from a customer to a financial institution, from a financial institution to a regulator, or from a regulator back to the private sector, accountability should travel with it.

A Practical Test for the Future

My experience leaves me with a simple proposition: Do not ask only whether information was shared. Ask what the information changed.

- Did it change a control?
- Did it trigger an investigation?
- Did it produce remediation?
- Did it prevent recurrence?
- Did it improve supervision?
- Did it strengthen consumer confidence?

If the answer cannot be demonstrated, the system may have achieved information exchange without achieving information effectiveness.

“The future of public-to-private information sharing should therefore be measured not by how much information institutions can collect or transmit, but by how effectively the ecosystem can turn information into accountable action, verifiable remediation and institutional learning.”

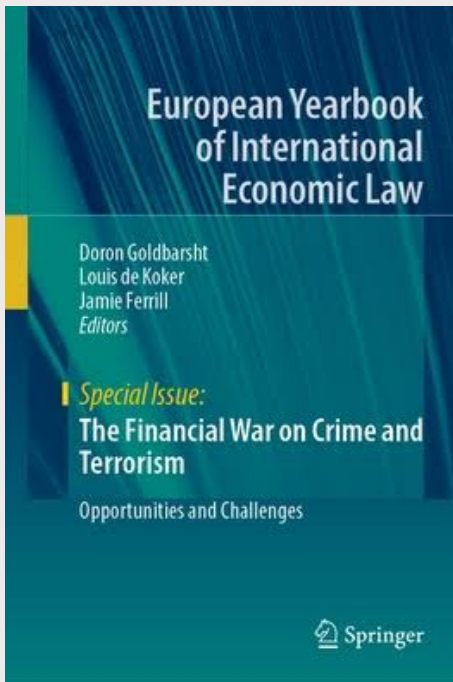
The strength of a financial system is not demonstrated only when everything works as expected. It is demonstrated when something goes wrong, and the system is capable of remembering, responding, correcting and learning. Information should move. But accountability must move with it.

Adam Kheri Famao



RESEARCH AT FIH

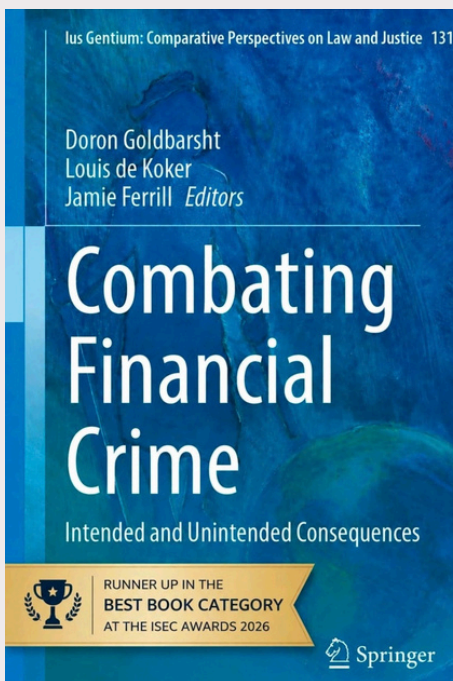
THE FINANCIAL WAR ON CRIME AND TERRORISM: OPPORTUNITIES AND CHALLENGES (2026)



A product of the FIH, this book critically examines global AML/CTF vulnerabilities and proposes innovative solutions to combat illicit activities. It examines the systemic nature of financial crime, covering topics such as AML leadership challenges, gaming sector exploitation, AI in crime detection, wildlife trafficking financing, and opportunities in public-private and private-to-private information sharing. Through case studies and analysis, it provides practitioners, policymakers, and academics with knowledge to prevent, detect, and mitigate financial crime, fostering a more secure and transparent global financial system.



COMBATING FINANCIAL CRIME: INTENDED AND UNINTENDED CONSEQUENCES (2026)



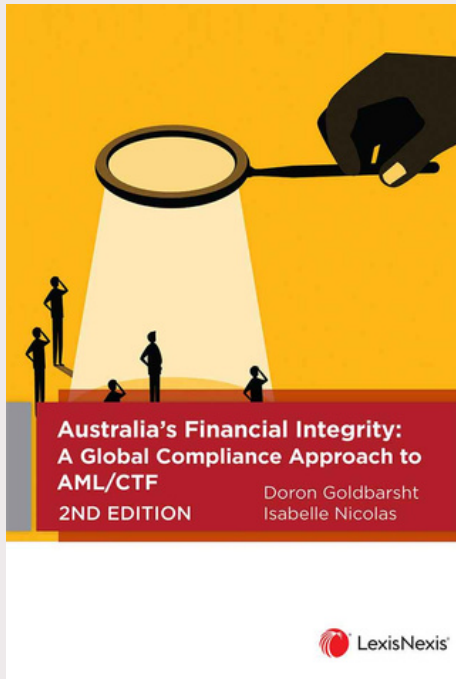
A product of the FIH, this book examines the ethical dilemmas and practical challenges faced by policymakers, practitioners, and the public as they navigate the evolving landscape of AML/CTF regimes. Drawing on analysis and real case studies, the book highlights how increased surveillance, regulatory controls, and new technologies may inadvertently undermine civil liberties. It assesses the impact of regulatory frameworks on vulnerable populations, non-profit organisations, and businesses, revealing the unintended consequences of policies designed to combat financial crime. By engaging with these challenges, the book calls for a more nuanced approach to financial crime control, one that protects society without undermining its core values.





RESEARCH AT FIH

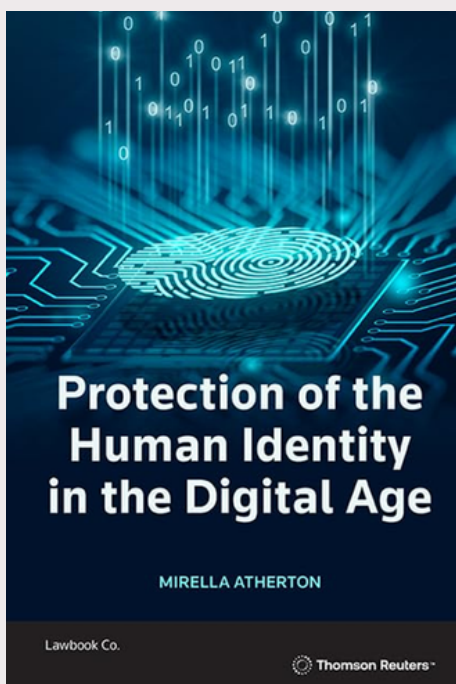
AUSTRALIA'S FINANCIAL INTEGRITY: A GLOBAL COMPLIANCE APPROACH TO AML/CTF (2nd ed, 2026)



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 into practitioners and students.



PROTECTION OF THE HUMAN IDENTITY IN THE DIGITAL AGE (2025)



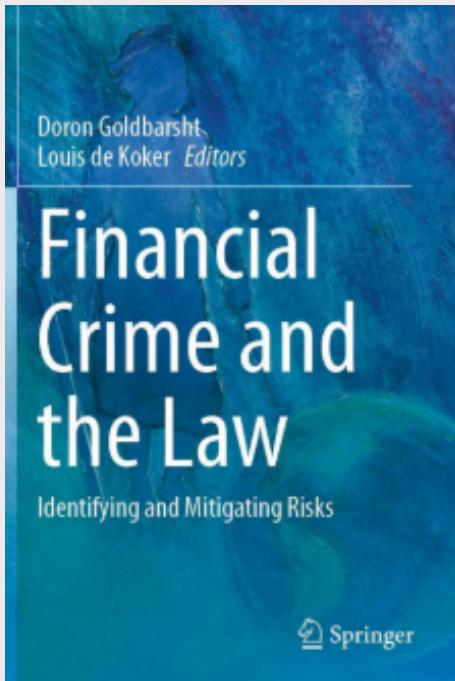
Written by Mirella Atherton, this book examines how digitalisation, artificial intelligence, big data, and global connectivity are reshaping concepts of privacy, autonomy, and security. The book examines how human identity and mass data collection intersect. It begins with a theoretical insight into privacy, surveillance and the harmful effects of unwanted intrusion, before examining the impact of mass surveillance and data security. Mirella explores the types of sensitive personal information that can be collected from human beings, including financial information. Offering a multidisciplinary perspective, it provides valuable insights for policymakers, academics, and practitioners navigating the intersection of technology, human rights, and identity protection.





RESEARCH AT FIH

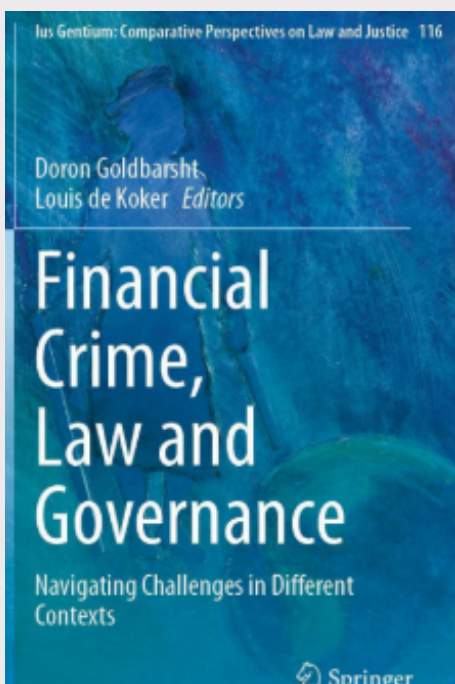
FINANCIAL CRIME AND THE LAW: IDENTIFYING AND MITIGATING RISKS (2024)



A product of the FIH, this collection, edited by Doron Goldbarsht and Louis De Koker, explores key issues in financial crime, including cryptocurrency 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 the 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 (2024)



A product of the FIH, 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.



FIH PODCAST



Listen to us on Spotify!

Season 3 of the *Financial Integrity Hub* Podcast

The Financial Integrity Hub produces a regular podcast series featuring speakers with financial crime and compliance expertise. Each episode 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 – Payment Systems and Financial Crime, with Toby Evans



Episode 2 – Anti-Money Laundering and Asset Recovery, with Jeffrey Simser



Episode 3 – Financial Crime and Financial Inclusion: An African Perspective, with Vivienne Lawack



Episode 4 – Sanctions in Practice: Design, Compliance, and Geopolitical Complexity, with Claudine Lamond



Episode 5 – Rethinking AML/CTF Effectiveness, with David Lewis



Episode 6 – Following the Money to Environmental Crime, with Richard Parlour



NEW! Episode 7 – International Anti-Corruption Court, with Allan Rock

In the latest FIH Podcast episode, Dr Hannah Harris is joined by Allan Rock, former Canadian Minister of Justice and Attorney General, and Chair of the Drafting Committee for the proposed International Anti-Corruption Court (IACC). They discuss the case for the IACC, why existing mechanisms often struggle to hold powerful actors accountable, and what stronger international cooperation could mean for tackling corruption and the movement of illicit wealth.

Thank you to our podcast partner – Arctic Intelligence!

Arctic Intelligence is a multi-award-winning RegTech firm specialising in financial crime risk, audit, and compliance software. Trusted by regulated businesses in over 25 countries, Arctic Intelligence delivers highly configurable, cloud-based AML/CTF and financial crime risk assessment platforms and content that help organisations better identify, assess, and manage financial crime risks.





FINCRIME & CULTURE

Rinsed: From Cartels to Crypto – How the Tech Industry Washes Money for the World's Deadliest Crooks

Review by Madeleine Olney, FIH Intern

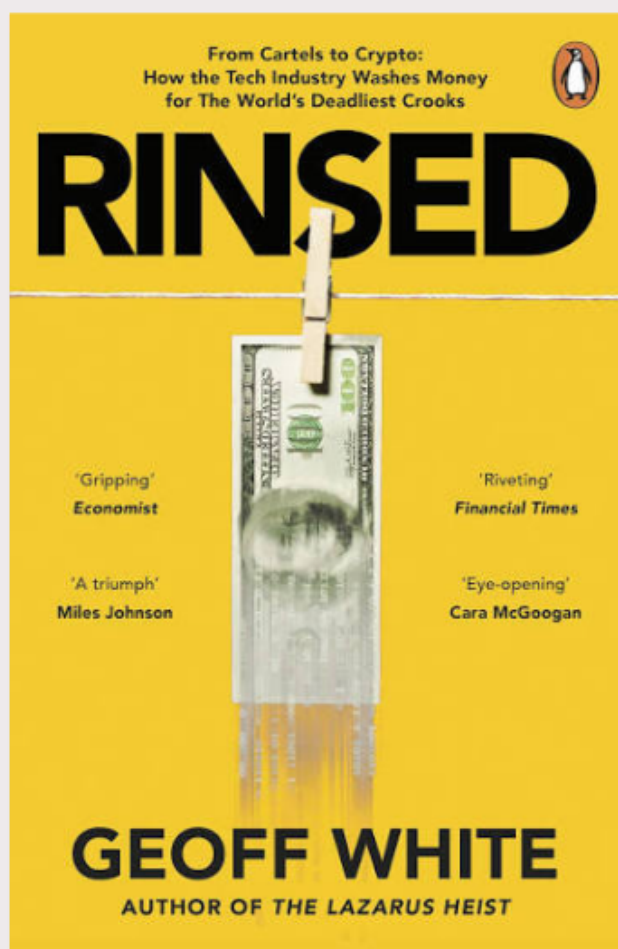
An explosive true-crime investigation into the hidden world of cybercriminals, cartels and the digital money laundering networks connecting them.

Geoff White's *Rinsed* takes readers deep into the rapidly evolving world of high-tech money laundering, revealing how organised crime has embraced technology to move, disguise and legitimise illicit wealth. Drawing on real cases, investigative reporting and interviews with people close to the criminal and investigative worlds, White traces the journey of dirty money across the globe, from traditional criminal networks to cryptocurrencies, online platforms and sophisticated digital laundering systems.

What makes *Rinsed* particularly compelling is its exploration of the unlikely intersection between organised crime and technology. White examines how criminals and cybercriminals increasingly work together, creating sophisticated networks capable of moving illicit funds across jurisdictions and through multiple layers of the financial and digital ecosystem. The book covers cases involving crypto, money mules, fraud networks, cybercrime and other emerging forms of financial crime.

For anyone working in financial crime, AML/CTF, cybercrime or law enforcement, *Rinsed* offers an accessible and engaging look at where financial crime is heading—and why traditional approaches to detecting and disrupting illicit finance may no longer be enough.

A gripping, eye-opening exploration of the blurred lines between technology, organised crime and financial crime.





FINANCIAL CRIME FILES

Recent Judicial Developments

Lucas Tulich, FIH Intern

BANO PTY LTD V AUSTRALIAN SETTLEMENTS LIMITED [2026] FCA 932

Bano Pty Ltd, a financial technology company, sought an urgent injunction to prevent Australian Settlements Limited from suspending its payment services. The application followed an AML/CTF review that raised concerns about Bano's cryptocurrency-related payment flows, "nested" arrangements that limited visibility over underlying customers, and the adequacy of its AML/CTF controls.

The Court dismissed the application, finding that Bano had established a prima facie case, but that it was weak and the balance of convenience strongly favoured refusing the injunction. In particular, the Court accepted that continuing to provide services to Bano exposed the respondent to real regulatory, reputational and counterparty risks, including the possibility that other financial institutions could restrict their dealings with it because of perceived AML/CTF risk.

Key Takeaway: Courts may be reluctant to require a financial institution to continue a relationship where a customer poses an unacceptable AML/CTF risk, particularly where supported by clear evidence.

MERCIFUL GROUP INC V NORFINA LTD T/AS SUNCORP BANK [2026] NSWCA 155

Merciful Group, a charity providing humanitarian aid across Lebanon, Syria and Yemen, challenged Suncorp Bank's decision to close its account under cl 15.2.

Merciful sought declarations that Suncorp breached the agreement and an injunction preventing the closure. Suncorp's decision followed enhanced due diligence that identified several risk indicators, including repeated transaction monitoring alerts, transfers involving high-risk jurisdictions, more than \$28 million sent to a third-party remitter, a sharp increase in donations, and donor names linked to organised crime.

Despite weaknesses in the drafting of Suncorp's closure clause, the Court dismissed the appeal, finding that the clause allowed termination to protect the bank's legitimate interests. While there was no finding that Merciful engaged in ML/TF, the Court upheld the termination as rational, honest and reasonable.

Key Takeaway: AML/CTF risk can provide a legitimate basis for terminating a customer relationship where the bank's contractual terms permit closure.

PULEO V BENDIGO AND ADELAIDE BANK LTD [2026] VSC 513

The Victorian Supreme Court considered Bendigo Bank's decision to close accounts linked to Gotham City, a licensed Melbourne brothel. Under its AML/CTF Program, the Bank classified brothels and sex work agencies as high-risk customers requiring enhanced customer due diligence. However, it did not impose a blanket ban on providing banking services to these businesses. The plaintiffs challenged the account closures, alleging discrimination, breach of contract and a failure by the Bank to provide financial services efficiently, honestly and fairly.

The Court dismissed all claims, finding that the Bank's risk assessment provided a rational basis for the closures, including irregular account activity, substantial cash withdrawals and transaction patterns consistent with potential layering. The Court also found that the plaintiffs' occupation was not, in substance, the reason for the closures.

Key Takeaway: Banks may close accounts to manage AML/CTF risk where the decision is supported by a rational risk assessment and the contractual terms permit closure.



3 UNDER 30 EVENT

DRIVING THE FUTURE OF FINANCIAL INTEGRITY

Thursday, 29 October 2026 | 6:30–8:00 pm
Sydney CBD

Following the success of our inaugural 3 Under 30 event in 2025, FIH is proud to bring the initiative back for its second year, celebrating three exceptional professionals under 30 who are making their mark in the fight against financial crime.

Bringing together emerging talent from industry, government and academia, the event provides a platform to hear their experiences, insights and perspectives on the future of financial integrity.

Join us to recognise the achievements of the next generation of financial crime professionals, hear what motivates their work, and gain fresh perspectives on the challenges and opportunities shaping the AML/CTF landscape. The evening will also provide an opportunity to connect with established and emerging leaders across the financial crime community.

Proudly supported by FIH, AUSTRAC and TOM.

For tickets, please visit the Financial Integrity Hub website or scan the QR code.



FIH ON TOUR MELBOURNE 2026

Thursday, 19 November 2026 | 6:00–8:00 pm

KordaMentha – 525 Collins St, Melbourne VIC 3000, Australia

After four years of End-of-Year Events in Sydney, the Financial Integrity Hub is heading to Melbourne. Join us for an evening bringing together leaders from government, industry and academia for networking and a panel discussion on key financial crime issues. The evening will also feature the 2026 Financial Crime Fighter of the Year Awards, recognising outstanding contributions to the fight against financial crime.

For tickets, please visit the Financial Integrity Hub website or scan the QR code. Early bird tickets available until 30 September, or until the allocation sells out, whichever comes first.



With thanks to our hosts:

KordaMentha



PREVIOUS EDITIONS



Regulating the Gatekeepers
June 2026



CTF and Violent Extremism
March 2026



Financial Crime and Technology
December 2025



Sanctions
September 2025



Virtual Assets (VA) and VA Service Providers
June 2025



Information Sharing
March 2025



AML/CTF Reform Implementation
December 2024



National Risk Assessment
September 2024



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.

If you would like to contribute your op-ed for our future FIH Insights, please contact us (fih@mq.edu.au)

**FINANCIAL
INTEGRITY HUB**



MACQUARIE
University
SYDNEY · AUSTRALIA

Thank you to our partners for their support!



Arctic Intelligence is a multi-award-winning RegTech firm specialising in financial crime risk, audit, and compliance software.



Unmatched Compliance.
Zero Compromise.

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!