FINANCIAL INTEGRITY HUB INSIGHTS

Sanctions

September Issue 2025

FINANCIAL INTEGRITY HUB

MACQUARIE University
SYDNEY | AUSTRALIA

ISSN: 2982-3188

LEADERSHIP

Patron
Honourable Patricia Bergin AO SC

Director
Associate Professor Doron Goldbarsht

Associate Director
Isabelle Nicolas

Advisory Board
Armina Antoniou
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
Jeremy Moller
Tony Prior

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

Researchers
Giang Nguyen
Samuel Orchard
Ben Scott

Interns
Emmanuel Anyuon
Koleap Lim
Zashaal Shahid
Tanya Singh
Reem Naboulsi-Armanno

Citing reference: Financial Integrity Hub 'FIH Insights' (2025) 1(3) FIH, Sydney
<https://www.mq.edu.au/research/research-centres-groups-and-facilities/groups/financial-integrity-hub/engagement>.

ABOUT US

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

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

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

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

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

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

Follow us here:

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

TABLE OF CONTENTS

- **Guardians of Integrity: Sanctions, Proliferation Financing, and Australia's International Obligations**
- **Opinion Pieces**
  - Sanctions as a Tool Against Proliferation Financing
    David Shannon
  - Sanctions: Navigating Compliance in an Increasingly Complex Geopolitical Landscape
    Gail Carter
  - How do FATF Sanctions Actually Work?
    Charles Littrell
  - The Impact of Sanctions on Humanitarian Aid and Cross-Border Financial Flows
    Yehuda Shaffer
  - Canadian Sanctions and the Curious Case of a Very Large Airplane
    Jeffrey Simser
  - Targeted Financial Sanctions: A DEA Agent's Perspectives on the Financial Frontline of Transnational Crime
    David Tyree
  - Targeted Financial Sanctions in the EU AML/CTF Framework: From Policy to Practice
    Georgios Pavlidis
  - Beyond the Stablecoin Scare: Sanctions Evasion's Bigger Picture
    Kristofer Doucette
  - Targeted Financial Sanctions: A Call for Accountability and Reform in Global Compliance
    Sisira Dharmasri Jayasekara
  - Targeted Financial Sanctions: Effectiveness, Challenges and Unintended Consequences
    Dare Joseph Ayinde
  - Regulatory Sanctions for AML/CTF Non-Compliance: Background Case
    William Gaviyau
- **Research at FIH**
- **FIH Podcast**
- **Upcoming FIH Events**

GUARDIANS OF INTEGRITY

SANCTIONS, PROLIFERATION FINANCING, AND AUSTRALIA'S INTERNATIONAL OBLIGATIONS

Image: David Shannon with Claudine Lamond and Louis de Koker at the 2025 *Financial Integrity Hub* Financial Crime Symposium

Sanctions are non-military measures used to respond to matters of international concern. In Australia, they are primarily administered under the *Charter of the United Nations Act 1945* (Cth) and the *Autonomous Sanctions Act 2011* (Cth). Broadly, sanctions fall into two categories: (a) targeted financial sanctions, which freeze assets of designated persons or entities and prohibit the making of assets available to these individuals or groups; and (b) trade restrictions, which prohibit the import and export of certain goods, services or commercial activities with specified countries or regions.

These measures aim to prevent armed conflict, terrorism, human trafficking, and the proliferation of weapons of mass destruction (WMD), while simultaneously signalling international condemnation by imposing economic and reputational costs on perpetrators.

Why Sanctions Matter

Sanctions play a vital role in protecting the integrity of the international financial system and upholding global peace and security. For Australia, strong sanctions compliance ensures domestic practices align with international obligations, reinforcing its reputation as a responsible international actor. It safeguards Australian businesses, financial institutions, and individuals from inadvertently facilitating illicit trade or proliferation financing, while also demonstrating Australia's commitment to the global non-proliferation regime. Non-compliance exposes businesses to significant legal, financial, and reputational risks, including potential criminal liability.

The New DFAT Advisory Note (August 2025)

On 25 August 2025, the Australian Sanctions Office (ASO), a division of the Department of Foreign Affairs and Trade (DFAT), released an updated Advisory Note on Sanctions and Proliferation Financing. This note is directed at 'regulated entities', including government agencies, businesses, financial

institutions, and individuals subject to Australian sanctions laws, and it provides detailed guidance on compliance obligations and risk management practices. The Advisory Note highlights several core concepts and definitions. It explains that 'designated persons and entities' are those specifically listed under Australian sanctions laws and subject to financial sanctions or travel bans, with DFAT maintaining a Consolidated List for screening purposes. The advisory also defines 'proliferation financing' as the provision of funds or financial services for the manufacture, acquisition, possession, or transport of WMD and their delivery systems in violation of international or national law. Further, the concept of 'reasonable precautions and due diligence' is emphasised, requiring businesses to undertake measures such as customer screening, robust internal controls, and comprehensive staff training to avoid involvement in sanctioned activities. Finally, the advisory explains that 'sanctions permits' are licences issued by the Minister for Foreign Affairs authorising activities that would otherwise be prohibited, granted only when they align with Australia's national interest

Risk Factors and High-Risk Sectors

The DFAT Advisory highlights that proliferation financing risks arise across multiple dimensions, including customer risk factors, such as links to sanctioned countries or suspicious ownership structures. Product and service risks are also relevant, particularly in areas such as trade finance, correspondent banking, or the movement of dual-use goods. Geographic risks relate to operations in, or exposure to, high-risk jurisdictions, notably Iran or the Democratic People's Republic of Korea (DPRK). Transaction risks can involve complex routings, the use of front or shell companies, or unusual shipping routes. High-risk sectors identified in the Advisory include, trust and company service providers, dealers in precious metals and stones, virtual asset service providers (VASPs), maritime shipping, and academic or research partnerships.

Known Methodologies and Red Flags

Proliferators frequently misuse dual-use goods with both civilian and military applications, trade-based money laundering techniques such as false invoices or manipulated documentation, shell companies and intermediaries to obscure beneficial ownership, and cryptocurrencies or fintech platforms to layer and obfuscate funds. Other red flags highlighted in the Advisory include:

- unexplained use of transshipment hubs,
- reluctance to provide end-user certificates,
- overlapping business details with sanctioned entities, and
- inconsistent business profiles.

International and Domestic Frameworks

United Nations Obligations

Sanctions are one of the primary mechanisms through which the UN Security Council enforces its resolutions. Under United Nations Security Council Resolution (UNSCR) 1540 (2004), member states must enact laws to prevent the financing and acquisition of WMD, a responsibility implemented through targeted financial sanctions that freeze the assets of non-state actors involved in proliferation activities. UNSCR 2325 (2016) strengthened this framework by requiring states to impose trade restrictions and sanctions to prevent proliferation financing and secure sensitive goods and technologies. In addition, country-specific sanctions regimes - such as those directed at Iran under UNSCR 2231, and at the DPRK under UNSCRs 2270, 2371, and 2375 - require states to implement comprehensive trade bans and targeted financial sanctions to restrict proliferation activities. In practice, this means Australia is legally bound to reflect these obligations within its domestic sanctions laws.

FATF Standards

Financial Action Task Force (FATF) Recommendation 7 requires countries to implement targeted financial sanctions in compliance with UNSCRs on WMD proliferation, ensuring that Sanctions Lists are applied consistently worldwide. Beyond this, Recommendation 19 and FATF 'calls to action' urge jurisdictions to apply enhanced due diligence and countermeasures against high-risk jurisdictions. For example, the FATF currently requires countries to apply countermeasures against the DPRK and Iran, meaning that Australian firms must align their practices with DFAT's sanctions lists and related controls. In this way, sanctions act as the operational tool through which compliance with FATF obligations is achieved.

Australian AML/CTF Requirements

From 31 March 2026, reforms to the *Anti-Money Laundering and Counter-Terrorism Financing Act* 2006 (Cth) (AML/CTF Act) will explicitly integrate sanctions compliance into business obligations. Firms will be required to identify and assess proliferation financing risks, including systematic screening against DFAT's Consolidated Sanctions List. Enhanced due diligence will be mandatory for high-risk jurisdictions such as the DPRK and Iran, to ensure that financial institutions do not facilitate sanctioned transactions. Verification obligations will also require businesses to check customers and associated parties against sanctions designations, embedding sanctions compliance into the everyday processes of AML/CTF programs. These developments demonstrate that sanctions are no longer merely foreign policy instruments, but are now integral components of domestic regulatory compliance for financial institutions, asset managers, and service providers.

Conclusion

Australia's sanctions regime plays a pivotal role in protecting international security and preserving the integrity of the domestic financial system. The updated DFAT Advisory Note provides regulated entities with detailed guidance to identify and mitigate proliferation financing risks. Compliance demands rigorous due diligence, continuous monitoring, and adherence to international obligations under UNSCRs, FATF standards, and domestic AML/CTF reforms. For businesses and institutions, effective sanctions compliance is both a legal requirement and a protection against misuse for illicit purposes.

SANCTIONS AS A TOOL AGAINST PROLIFERATION FINANCING

David Shannon

The proliferation of weapons of mass destruction (WMD) and related financing poses a profound threat to international peace and security. Proliferation financing (PF) enables the acquisition of nuclear, biological, and chemical weapons, as well as their delivery systems, by actors seeking to develop or expand such capabilities. The financial sector, if exploited, can become a critical enabler for illicit procurement and related activities. Identifying and disrupting the financing of proliferation is therefore central to safeguarding the international community against the risks posed by WMD.

Targeted financial sanctions, embedded in the Financial Action Task Force (FATF) Recommendation 7, are designed to constrain the financial operations of designated individuals, entities, and groups deemed to threaten global peace and security. By restricting access to financial resources, such measures impair the ability of proliferators to procure illicit goods and technologies essential for WMD development. Countering proliferation financing (CPF) thus complements wider national and international efforts to prevent the spread of WMD and preserve international security.

FATF's Approach

The FATF employs a dual approach to combating PF, integrating a global mandate under United Nations Security Council Resolution (UNSCR) 1540 to prevent non-state actors from acquiring WMD, alongside country-specific obligations for targeted sanctions and countermeasures. Currently, the Democratic People's Republic of Korea (DPRK) is the sole state subject to UN sanctions under Recommendation 7.

Recommendation 7 requires countries to establish legislative and operational mechanisms to:

- freeze, without delay, assets owned or controlled, directly or indirectly, by designated proliferators;
- prohibit the provision of financial or economic resources to such persons or entities, except as authorised under the relevant UNSCR; and
- monitor and enforce compliance domestically.

Recommendation 2 further mandates national coordination to ensure effective implementation and risk understanding. Together, these measures form a cornerstone of the global non-proliferation framework. However, FATF's fourth round of mutual evaluations revealed persistent shortcomings in both technical compliance and effectiveness, with many jurisdictions struggling to implement targeted sanctions in practice. Enhancing compliance and effectiveness remains critical to denying proliferators access to the global financial system.

Recommendation 1 now requires countries to identify and assess the PF risks for the country, in particular the potential breach, non-implementation or evasion of the targeted financial sanctions obligations referred to in R.7. in practice many countries go further and consider the risks from wider aspects of PF. Recommendation 1 goes further and requires countries to share risk information with

the private sector (financial institutions, designated non-financial businesses and professions and virtual asset service providers (VASPs)). Those same categories of the private sector are obliged to prepare enterprise risk assessments for PF and implement both rules-based and complementary risk based measures.

Proliferation Financing and Sanctions Evasion

Despite comprehensive international frameworks, PF remains resilient, often facilitated through complex sanctions evasion schemes. Both state and non-state actors employ increasingly sophisticated methods to circumvent restrictions, including the procurement of dual-use goods, the use of transnational networks, and the exploitation of financial and trade systems.

As of June 2025, FATF identified four key typologies of PF and sanctions evasion: the use of intermediaries in third countries; concealment of beneficial ownership; exploitation of emerging technologies; and misuse of maritime and shipping sectors. These schemes are often supported by extensive corporate networks, front companies, and layered ownership structures designed to obscure links to sanctioned actors. Such activities present substantial challenges to both governments and financial institutions attempting to detect and disrupt illicit flows.

Mitigating Risks

Addressing these challenges necessitates vigilance, innovation, and international cooperation. Suspicious transaction reporting, coupled with robust sanctions screening, remains fundamental for detection. However, these measures must be supplemented by enhanced intelligence sharing across public and private sectors, inter-agency coordination, international collaboration, and the integration of advanced technologies such as blockchain analytics. Collaboration between governments and the private sector and academia offers the best avenue to improve guidance, advisories and granular risk information to improve the effectiveness of prevention, detection and enforcement actions against PF. Effective domestic frameworks for investigation and prosecution are likewise essential to deter and disrupt PF.

Assessing Compliance and Effectiveness – FATF's Global 5th Round

The FATF and the global network of FATF-style regional bodies (FSRBs), including the APG, have commenced the Global 5th Round of Mutual Evaluations to re-assess both compliance and effectiveness. This will assess the revised obligations in relation to PF risk assessments and all aspects of effectiveness of CPF measures. The first set of mutual evaluations will be published in late 2025 and will provide a clear view of the approach the FATF and FSRBs are taking to combat proliferation financing in changing and riskier global, regional and national contexts.

Conclusion

PF continues to evolve through the use of sophisticated evasion techniques and emerging technologies, undermining the effectiveness of targeted sanctions. Without strengthened CPF frameworks and coordinated public–private responses, illicit actors will continue to exploit systemic vulnerabilities. Building resilience through enhanced compliance, risk understanding, and international cooperation is indispensable for preserving the integrity of the global financial system and sustaining efforts to prevent the spread of WMD. Raising awareness of these issues is therefore a necessary step toward strengthening the global response to PF and sanctions evasion.

David Shannon, Director- Pacific Technical Assistance
Asia/Pacific Group on Money Laundering.

SANCTIONS: NAVIGATING COMPLIANCE IN AN INCREASINGLY COMPLEX GEOPOLITICAL LANDSCAPE

Gail Carter

Over the last twenty years, the world has experienced extensive and increased use of economic and trade sanctions as nation states and multi-lateral organisations, with differing political views and foreign policy objectives, have responded to shifts in international security and changing global trends. The need for, and effectiveness of sanctions, in an increasingly volatile international community are ongoing questions. However, the reality is sanctions have been, and remain, an important tool in the arsenal of governments around the world; they will remain. The consequences of getting it wrong when it comes to complying with sanctions laws are high. Terrorists may prevail where otherwise they would have been defeated, nuclear proliferation may continue to contribute to volatility where otherwise it could be controlled.

Sanctions are more targeted than ever before. The nature and volume of sanction programmes, issued by an increasing number of sanctioning regimes, means the landscape is more complex in nature, costly in terms of regulatory compliance and continues to result in unintended consequences.

Often debate spans a number of issues, such as the need for sanctions, whether or not they operate as intended or have harmful unintended consequences, whether they are effective, why there is such inconsistency between regimes of like-minded nations and evasion of sanctions (to name a few). These are all important issues and policy makers must continue to check and challenge each one. What does not get sufficient consideration is whether or not enough people actually know what sanctions are and, beyond that foundational question, if they understand the importance of complying with sanctions laws - and the consequences if they don't.

Those who have a heightened awareness about sanctions laws and regulatory compliance expectations, in Australia and overseas, understand very well, when it comes to compliance, there is no one size fits all. Key points for consideration are:

- Sanctions laws apply to everyone to varying degrees;
- The extent to which sanctions apply will depend on where in the world assessment is undertaken, who and what activities are involved;
- No one person or organisation can be responsible for sanctions compliance end-to-end;
- Some persons will play a more material role than others; and
- The type of compliance solution, where one is required, will vary significantly.

The age old adage of '*nature, size and complexity*', plays a material role in designing an appropriate compliance solution. Understanding the regulatory landscape relevant to individual or organisation activities is critical. The importance of a thorough risk assessment and a clear risk appetite position cannot be overstated. Understanding regulatory expectations is paramount. Designing a sustainable, fit for purpose solution subject to ongoing management and oversight, with regard to overlapping regulatory regimes, and demonstrable to regulators, is essential.

In recent years, concerted effort of like-minded western nations, working together to achieve individual foreign policy objectives, whilst addressing common matters of international concern, has been evident. A notable example of this is the ongoing application of sanctions by the United States, United Kingdom, European Union, Canada and Australia, against Russia's unlawful breach of Ukraine sovereign territory. Whilst each has different sanctions targets, many are common, and the collective objective of these nations has been to stop Russia's aggression. This assists businesses when designing compliance solutions and importantly supports each sanctioning regime in achieving objectives of the laws. The effort to align sanctions programmes as much as possible must continue; to minimise unintended consequences and regulatory compliance burden on businesses, communities and individuals.

Regulatory guidance has been much more forthcoming in recent years, further evidencing the ongoing commitment to the use of sanctions as tools of foreign policy and clarifying regulatory compliance expectations. Regulatory guidance, whilst not a necessary pre-cursor to enforcement, is a clear signal that a regulator intends to enforce compliance where expectations are not being met. The co-operation of like-minded nations in the design of policy is mirrored in the design of regulatory guidance and it's clear co-operation extends to oversight activities and enforcement for non-compliance.

Generally speaking, when it comes to sanctions compliance, the heavy lifting is done by businesses, either small, medium or large. That's reasonable and generally the way these types of laws play out. However, that doesn't mean individuals can be ignorant of their own obligations. All must actively understand their obligations in the context of numerous roles all have in day to day life. All need to share their awareness, understanding and experience in assessing and appropriately managing sanctions compliance in order to lift the collective consciousness and call to action.

The consequences through lack of awareness and inaction – and getting it wrong - are too high. No one wants to be 'that person' or 'that company' involved in funding terrorist activities through the simple act of a donation, through the systemic processing of international payments to terrorist organisations or anything akin to such egregious behaviour. The time to understand sanctions compliance obligations, no matter 'who' you are, is right now.

Gail Carter, Economic and Trade Sanctions Specialist, Executive Director of KordaMentha.

HOW DO FATF SANCTIONS ACTUALLY WORK?

Charles Littrell

Since its 1989 founding, the Financial Action Task Force (FATF) has successfully induced widespread compliance with its technical standards, and increasing compliance with its assessments of effectiveness. The FATF defines its mission as: (a) Identifying the methods and trends used to facilitate financial crime; (b) Setting global standards for technical compliance and effectiveness of national jurisdictions combatting financial crime; (c) Assessing national jurisdiction implementation of these standards; and (d) Identifying high risk jurisdictions which are either falling short on implementation (the "grey list") or refusing to cooperate with the FATF (the "black list").

The great majority of the world's jurisdictions (excluding Iran and North Korea) have stated that they are willing to comply with the FATF's standards. Furthermore, there is considerable evidence (including many articles in *FIH Insights*) that most countries in fact devote considerable resources to meeting these standards. This is a curious outcome, because there is no evidence that by meeting the FATF's standards, any jurisdiction will actually reduce financial crime. There is on the other hand ample evidence that there are massive costs associated with the global financial crime fighting regime. Furthermore, there is increasing evidence that the FATF's national assessments are unjustifiably biased in favour of rich, white majority countries, and against poor, black majority countries.

This leads to a conundrum: How does a self-appointed international organisation without any formal sanctions powers ensure near-universal compliance with standards that are widely and increasingly seen as almost comically ineffective, not to mention crushingly expensive and probably racist?

It turns out that the answer to this conundrum is simple: appearing on the FATF's grey list may materially complicate US Dollar (USD) clearing access for banking systems in the named jurisdictions. Given the architecture of the global financial system, limited, and in the worst case, closed access to USD clearing can be catastrophic for affected jurisdictions. This extends well beyond the banking system, to participation in goods and services imports and exports. Even if a country has ample funds to purchase imports, making these purchases is much harder without access to USD clearing.

This constraint does not apply to American banks, which enjoy direct access to USD clearing via their domestic Fedwire payments facility. Given that the United States demanded the initial creation of the FATF and has been the most prominent force for the FATF's growing influence over time, it is curious that the FATF's only constraining mechanism does not apply to American banks or the American financial system. Fedwire payment fees are typically less than USD 0.10 per transaction.

International banks must use American banks to act as correspondents to clear their USD payments. The correspondent bank clearing fees range from a few dollars for routine retail transactions, to several hundred dollars for more complex transactions, particularly for jurisdictions featuring on the FATF grey list.

Leaving aside the increased cost, FATF grey-listed and particularly black-listed countries face the risk of not being able to secure correspondent banking services for USD clearing. Many countries have closely integrated their economies with American trade flows. Grey listing can complicate payments and financing for these trade flows, and black listing can end them. There is an accordingly large incentive for countries to comply with the FATF's standards, even though they have no force in law.

Why would American banks become reluctant to serve as correspondent banks for USD clearing in jurisdictions subject to the FATF's grey listing?

Because American bank regulators frequently apply large fines and other sanctions to banks that are alleged to be deficient in their financial crime controls, and insufficient attention to "customer of our customer" risks in correspondents can be a material factor in determining the scale of these punishments. There is also the consideration that U.S. banks are largely prohibited from dealing with banks and payments from FATF blacklisted countries. There is a broad perception that being placed on the FATF grey list is bad for a nation's economic prospects, but slipping from the grey to the black list is something of an economic death sentence for countries which are unwilling to become rogue states.

FATF grey listing increases the risk of "de-risking", about which much ink and angst has been spilled in recent years. Other than the obvious outlier cases of Iran and North Korea, and recent issues with Myanmar, over 100 countries have featured on the FATF grey list, but few have made the black list. The main reason this is the case is that the catastrophic costs of black listing means that countries falling onto the grey list have a very large incentive to toe the FATF line, and improve the assessment of their adherence to the FATF's standards.

Where do we go from here? The author is unaware of any material discomfort from the FATF or American officials with what is an obviously ineffective international regime to combat financial crime. It doesn't work, it is very expensive, and it is mired in bias and hypocrisy. From all indications, it will stay that way. The threat of loss of USD clearing is likely to remain an insurmountable constraint for non-American jurisdictions; so nearly all these jurisdictions will continue to comply on some basis with what we are all beginning to understand is a woefully unsatisfactory global regime for financial crime suppression.

Charles Littrell, Former EGM of the Australian Prudential Regulation Authority, Former Inspector of Banks and Trust Companies for the Central Bank of The Bahamas, and Founder of the International Research Conference on Empirical Approaches to Anti-Money Laundering.

THE IMPACT OF SANCTIONS ON HUMANITARIAN AID AND CROSS-BORDER FINANCIAL FLOWS

Yehuda Shaffer

Recent events in Gaza require both national authorities and sanction practitioners worldwide to update their risk understanding of potential terror related targeted financial sanctions (TFS) circumcision typologies, and introduce new mitigation measures to prevent terrorist financing (TF) through the abuse of Non-Profit Organisations (NPOs) by terror groups using financial flows disguised as humanitarian aid. Recently, the US Office of Foreign Assets Control (OFAC) sanctioned several sham charities that are prominent financial supporters of Hamas's Military Wing and its terrorist activities, responsible for TF under the pretence of conducting humanitarian work, both internationally and in Gaza. These designations follow other designations by Australia and the UK targeted at Hamas financial facilitators.

Both Hamas and the Popular Front for the Liberation of Palestine (PFLP) have long abused the trust of the international community and public support for legitimate humanitarian causes, to fund their terrorist activities and bring violence to the Israeli and Palestinian people. These new designations are targeting terrorists and terrorist organisations that seek to abuse the NPO sector to raise funds under the façade of humanitarian support.

What recent events have taught us is that TF risks still exist, primarily in the context of areas controlled geographically by terror groups where humanitarian aid is being distributed, and through the use of sham charities. This includes terrorist networks that establish seemingly legitimate NPOs under the guise of providing humanitarian assistance, but instead are primarily utilised for funnelling money to terrorist organizations, including through the sale of goods supplied to them as humanitarian aid.

Some measures can effectively be used to mitigate these emerging risks:

1. One such measure should be considering all designations made by various jurisdictions (for example by Israel) according to UNSCR 1373, even if these are not legally binding. A potential hit on such lists of third countries may not legally warrant the freezing of the assets in a specific jurisdiction, but at minimum, should require reporting a suspicious transaction report (STR) where a suspicion of TF exists.
2. A second measure to apply is strict customer due diligence (CDD) of the local partners involved in the distribution of humanitarian aid in an area of conflict. Applying the Know your Local Partner (KYLP) rule will minimise the potential abuse of the charitable sector by terrorists like Hamas and the PFLP, who continue to leverage sham charities as fronts for funding their terrorist and military operations.
3. A third mitigating measure should be the mandatory use of regulated channels for the transferring of the funds, and in no case agree to the use of cash, to prevent terrorist actors from exploiting the humanitarian situation to fund their violent activities at the expense of their own people. While this is extremely difficult in areas of conflict, the assumption must always be that cash will be most probably diverted to TF and other methods including using technology (i.e. biometric prepaid cards) should always be considered.

OFAC Guidance

The inherent tension between the need to provide humanitarian assistance in areas of conflict, and the obligation to prevent TF, was brought under a spotlight right after the Hamas attack on Israel 7/10 when OFAC published guidance for the Provision of Humanitarian Assistance to the Palestinian People. The guidance emphasised, on one hand, that the US remains committed to denying Hamas access to funds following its heinous terrorist attacks against the people of Israel, while also ensuring legitimate humanitarian aid can continue to flow to the Palestinian people in Gaza.

In this guidance, OFAC encouraged donations be made only to trusted organisations and, given the unique risk of Hamas financing, OFAC encouraged donors to conduct appropriate due diligence to ensure their donations are being received by legitimate organisations, including by searching the Specially Designated Nationals (SDN) List and paying attention to the red flags published by FINCEN, such as:

- checking the nexus to identifiers listed for OFAC-designated entities, to include email addresses, physical addresses, phone numbers, or passport numbers, or virtual currency addresses,
- transactions with a Money Services Business (MSB) that operate in higher risk jurisdictions tied to Hamas, and are reasonably suspected to have lax CDD requirements, opaque ownership, or otherwise fails to comply with AML/CFT best practices.
- links to 'trading companies', or other companies that have a nexus with Iran or other Iran-supported terrorist groups, such as Hizballah and Palestinian Islamic Jihad.

Abuse of the NGO Sector

Terrorists have a long history of abusing the NPO and charitable sectors. Some of these NPOs and charities are entirely co-opted and run by these designated terrorists, with their links to terror intentionally obscured in order to evade sanctions. This allows terrorists to exploit the sympathy and generosity of the international public at the expense of the people in need.

For this reason, in 2001, FATF broadened the TF definition to include any person who provides or collects funds with the knowledge that they are to be used, in full or in part by a terrorist organisation or by an individual terrorist (even in the absence of a link to a specific terrorist act or acts). For example, providing aid to a charity run by a terror group would be criminalised. Unfortunately, and contrary to this, in a recent document issued by the Council of Europe on the definition of terrorism, the importance of safeguards and exemptions for humanitarian actors and other legitimate activities, was emphasised, which could create a significant loophole for terrorists to abuse.

What Should Governments and Practitioners Do?

Governments and sanctions practitioners should:

- educate themselves on emerging TF risks,
- apply mitigating measures focusing on all relevant UNSCR 1373 terror related designations (even if not in force in a specific jurisdictions),
- apply the KYLP rule to anyone operating in areas of conflict which might be subject to terror,
- use only regulated channels for the transferring of the funds to these areas,
- strictly forbid the use of cash, and
- develop technological tools, such as biometric prepaid cards for the distribution of humanitarian aid.

Yehuda Shaffer, Founder of the Israeli FIU and Former Israeli Deputy State Attorney (Financial Enforcement).

CANADIAN SANCTIONS AND THE CURIOUS CASE OF A VERY LARGE AIRPLANE

Jeffrey Simser

A Soviet-era cargo plane, an Antonov An-124, sits on a conspicuous corner of the tarmac at Canada's largest international airport in Toronto, and is the subject of widely watched precedent-setting litigation that will test a government's ability to forfeit sanctioned assets.

In May 2022, Canada amended their sanctions regime to allow for the forfeiture of property owned, held or controlled by a sanctioned entity. The government is not required to show that the property was involved in a sanctioned entity. The government is not required to show that the property was involved in a sanction violation or was a traceable proceed of such a violation. Other countries, particularly in Europe, faced seemingly intractable rule of law problems: one moment, an asset was legally held; then following a political decision, the asset was forfeitable. Canada effectively brought the forfeiture of sanctioned property into an uncharted territory and allies are watching this contested litigation closely.

Canada relies on three primary sanctions statutes, a Magnitsky Act, a statute to enforce sanctions imposed by the United Nations and the *Special Economic Measures Act (SEMA*). SEMA is the sanctions workhorse, operating largely through regulations passed by cabinet. SEMA can only be used against privately held assets; the State Immunity Act is not overridden by the statute. Like most Western countries, Canada has a sanctions list with 5,074 entries at the time of writing (many hailing from Russia, Iran, North Korea and Belarus). Canada has frozen CDN $185 million in assets and blocked $473 million in financial transactions. Canada's financial intelligence unit, FINTRAC, has a mandate to detect, prevent and deter sanctions evasion which applies to roughly 31,000 reporting entities, including financial institutions.

In June of 2024, FINTRAC issued a special bulletin on sanctions evasion advising reporting entities to be wary of intermediary jurisdictions, import/export control evasion, opaque corporate structures, non-resident banking, proxies, enablers and virtual currencies. SEMA gives the Minister and Cabinet authority to seek information and assistance from a broad variety of governmental bodies, including Canada's espionage service (the Canadian Security Intelligence Service) and its eavesdropping agency (the Communications Security Establishment). Deliberations in cabinet, where a forfeiture decision will effectively be made, are made in secret and protected by executive council privilege.

In 2022, the Antonov-An 124 owned by the Irish subsidiary of a Russian cargo company, landed at Toronto's Pearson International airport. This is the world's largest civilian cargo aircraft, with a lift capacity of 150 tons. The Antonov was carrying 60,900 kilograms of COVID-19 rapid test kits from Tianjin, China.

The Canadian government had sought assistance from the civil aviation authority in China to ensure that the plane would have the necessary flight and export permits. While the plane was still being unloaded, Canadian airspace was closed to Russian aircraft in response to the unjustified invasion of Ukraine. Just over a year later, on April 5, 2023, the owners of the plane were listed under SEMA's sanctions regime.

Image: Russian Antonov An-124 cargo at Toronto Pearson International Airport (YYZ).

On June 8, 2023, a SEMA order-in-council was issued by Cabinet ordering the seizure of the plane. In February of 2024, the sanctions listing was amended to include corporate entities associated with the airplane, including an Irish subsidiary. In March of 2025, a non-conviction forfeiture proceeding was launched against the airplane. Litigation and an arbitration hearing have ensued. The airplane's beneficial owners have made several claims in federal court: they initially asserted that four people not on the sanctions list own the plane (the government revised the sanctions listing in response). The owners claim that their company supports peacekeeping and humanitarian missions. They disavow any connection to the Putin regime or the Russian Wagner mercenary group (although Russian regime has threatened to retaliate against Canada as a result of this case). The owners claim that the airplane has been sitting on the tarmac, in its prominent parking spot, suffering from exposure through Canadian winters without receiving any maintenance whatsoever. The founder and former CEO of the cargo plane's parent company is Alexey Ivanovich Isaykin (a former Soviet air force officer). Government officials have referred to Isaykin as a Russian oligarch and claimed that the company was complicit "in Putin's war of choice".

This litigation will likely navigate some intriguing legal issues. On paper, SEMA appears to have elided some of the legal and rule of law challenges that allies have identified in their own countries. Canadians are constitutionally protected from unreasonable search and seizures. In terms of due process, SEMA decisions are made secretly, in cabinet. Individuals and entities that are sanction-listed are not given reasons or notice. While there is a reason for this - if a sanctioned entity had notice, it is likely they

would move the asset outside of Canada – the designation process is completely opaque. Assets are frozen with clear retrospective effect. Canadian courts have consistently held that statutory enactments that impact the rights of a citizen are presumed not to have retrospective effect. While there are exceptions, the legislation needs to be emphatically clear about retrospective application (and SEMA may not be). The policy beneath the doctrine against retrospectivity is sensible, citizens ought to be able to organize their relationships and affairs properly with a view to the state of the law.

In addition to litigation in Canadian courts, there's an on-going arbitration hearing in Singapore. Canada has signed a series of bilateral investment treaties, generally referred to FIPAs or Foreign Investment Protection Agreements. In 1989, as the Soviet Union began what became an irreversible decline, Canada signed a FIPA with the USSR. Investments under the treaty include any kind of asset. Canadian investors were no doubt concerned with the possibility that a communist government would arbitrarily expropriate Canadian free enterprise assets held in Moscow and elsewhere, so the treaty has fairly strong provisions prohibiting expropriation of assets without adequate compensation. Ironically, Canada may be hoisted on the petard of concerns it had decades ago about a Russian government. The owners of the cargo plane have announced that they will seek an arbitration, claiming $100 million in compensation from Canada under this treaty. A three member arbitration board has been established in Singapore to hear the case.

This case is the first time that Canada has exercised SEMA's forfeiture powers. G7 countries and Ukraine's allies will watch this matter closely. If Canada does succeed, they have committed to work directly with Ukraine to redistribute assets as compensation for human rights abuses. A Canadian failure may impact the latitude other governments have to visit consequences in sanctioned assets. Meanwhile, motorists leaving the airport for downtown Toronto cannot miss the massive plane parked on the corner of the tarmac.

Jeffrey Simser, Asset Forfeiture Law, Former Legal Director of the Ministry of the Attorney General, Canada, Senior Associate at Royal United Services Institute and Canada's first Director of Civil Asset Forfeiture.

TARGETED FINANCIAL SANCTIONS: A DEA AGENT'S PERSPECTIVES ON THE FINANCIAL FRONTLINE OF TRANSNATIONAL CRIME

David Tyree

Throughout my 25-year career with the United States Drug Enforcement Administration I had the opportunity, and the burden, of standing on the financial frontline of transorganised crime. From the islands of Cape Verde, West Africa to the streets of Lisbon, Portugal and throughout Europe, I witnessed firsthand how organised criminal networks adapt, evolve, and exploit global systems for financial gain. My role extended beyond traditional narcotics investigations; it demanded collaboration with international law enforcement, intelligence agencies, and crucially, entities within the U.S. Department of the Treasury, including the Office of Foreign Assets Control (OFAC). One of the most powerful tools in our arsenal was the use of targeted financial sanctions. That being said, sometimes having the most powerful tool only matters if the timing is right. I know from personal and professional experience—using a high-powered electric saw too early or too late in a project can do much more harm than good.

Targeted financial sanctions, particularly those imposed by OFAC under the *Kingpin Act* or executive orders addressing global threats, are often misunderstood. To the average observer, freezing bank accounts and blacklisting entities may seem like bureaucratic formalities or an "after-action" at the end of an investigation. However, for those who've spent their careers targeting narco-traffickers, money launderers, and terror financiers, these sanctions represent precision-guided missiles in a financial warzone, and they can have real impact and felt consequences.

Effectiveness: Cutting the Head off the Financial Snake

At its core, a targeted financial sanction aims to deprive criminal organisations of access to the international financial system, and hopefully, their ill-gotten gains. When implemented effectively, a sanction can freeze assets, prohibit U.S. persons and institutions from doing business with designated individuals or entities, and serve as a public declaration of "criminal actor" that reverberates through the global banking community and communities at large.

During my time in West Africa, we targeted a criminal network that trafficked cocaine from South America through Africa and into Europe. The group's leadership had sophisticated laundering mechanisms, including front companies in logistics, real estate, and trade-based finance. They also relied on shell corporations registered in multiple jurisdictions and used bank accounts spread across three continents. When OFAC designated the network's leaders and their businesses, the impact was swift and profound. Bank accounts were frozen around the world. International partners began conducting their own domestic investigations.

Legitimate companies, fearful of reputational damage or secondary sanctions, severed ties overnight. In effect, the designation didn't just cut off access to money; it destabilised the organisation's entire operational infrastructure. This is the result of when the good guys "follow the money" and ultimately "action the money." This criminal network couldn't pay couriers, bribe officials, acquire weapons or pay for narcotics.

That is the power of targeted sanctions: not just the disruption of a criminal network, but essentially preventing them from accessing the financial backing required to maintain and sustain operations.

Challenges: Enforcement, Evasion and Global Compliance

Still, sanctions are only as effective as their enforcement; and therein lies the challenge. Unlike a physical arrest, a sanction does not restrain the subject. It restricts their financial maneuverability, but it also demands constant vigilance and international cooperation to maintain pressure. The burden falls on many in the law enforcement, intelligence, and financial industries.

Criminal organisations are adaptive. Once a designation is issued, if not already using proxies, sanctioned individuals often shift to using nominees or third-party intermediaries. Shell companies are restructured. Funds are routed through informal value transfer systems like hawala networks or nested correspondent banking arrangements. Cryptocurrencies, which offer pseudo-anonymity and cross-border liquidity, add another layer of complexity. I've seen OFAC-designated traffickers reinvent themselves within weeks, aided by complicit enablers and jurisdictions with weak regulatory oversight.

In Europe, some countries struggled to act on US designations due to conflicting legal standards or political reluctance. Even when sanctions were multilateral, coordinated through the United Nations or European Union, differences in implementation diluted their impact. And in some parts of Africa, the lack of technical capacity and limited access to real-time sanction lists meant that enforcement was effectively nonexistent.

Moreover, for US financial institutions tasked with compliance, the risk of inadvertently violating sanctions is immense. They must navigate name-matching algorithms, sift through opaque ownership structures, and interpret ambiguous designations—often in real time. I had the opportunity to audit the OFAC program at a major financial institution. Although the Financial Crimes Unit involved in the OFAC program did an outstanding job, some bad guys aware of their OFAC designation changed their identifying information enough to pass through the controls undetected. While OFAC provides guidance, the practical burden of compliance falls on banks, which must balance regulatory expectations with the realities and demands of international finance.

Unintended Consequences: Collateral Damage and Innovation

Targeted financial sanctions are scalpel-like in design, but sometimes the cut is deeper than intended. In my experience, collateral damage, particularly in developing economies, is a real concern. Take, or instance, a logistics company in West Africa that was sanctioned due to its ownership by a member of the criminal organisation. The company handled imports for dozens of small retailers,none of whom had any connection to the criminal activity. When the business was blacklisted, these retailers lost their inventory supply chain Some folded. Innocent employees lost jobs. The broader community, already economically fragile, suffered unintended consequences.

There's also a darker irony at play: sanctions can sometimes drive criminal networks into more clandestine methods of operation. When formal banking channels become inaccessible, groups turn to cash smuggling, underground banking, and digital currencies. These methods are harder to detect, disrupt, and often fall outside traditional compliance frameworks.

Furthermore, the "scarlet letter" of a sanctions designation can have geopolitical implications. In some cases, sanctioned individuals find protection under hostile or indifferent governments, which view U.S. designations as instruments of foreign policy, rather than tools of justice. This can embolden the criminal networks and create new avenues for them to continue their illegal activity.

A Balanced Weapon in a Broader Strategy

Despite the challenges, I remain a strong proponent of targeted financial sanctions as part of a broader strategy to disrupt and dismantle transnational organised crime. These are complex problems which require complex solutions, and, in my opinion, putting too much faith into one solution reduces the efficacy of the combination of tools that exist as force multipliers. Sanctions work best when combined with robust financial intelligence, international cooperation, and follow-up enforcement.

They send a message, not only to the criminals but to their partners, service providers, and political protectors, that the cost of doing business with criminal organisations is too high, and justice can and should prevail.

In my current work supporting law enforcement and financial investigations through technology, I see firsthand how digital tools—like advanced bank data analysis platforms—can accelerate sanction investigations and support real-time interdiction. We can identify patterns of evasion, trace beneficial ownership, and provide actionable intelligence to law enforcement and regulators around the world.

Conclusion: Financial Warfare in the 21st Century

As the battlefield of crime expands beyond borders and into cyberspace, the importance of financial warfare cannot be overstated. The kingpins of today wear suits, not bandoliers. Their weapons are not just AK-47s, but spreadsheets and invoices generated by artificial intelligence and shell companies with a presence on social media. Sorting through it all can be like looking for a needle in a stack of needles. Targeted financial sanctions give us a fighting chance—not to eliminate crime altogether, but to tilt the balance towards the good buys. But like any weapon, they require precision, restraint, and continuous refinement. As a former DEA Special Agent who has seen the damage that unchecked financial crime can inflict on nations and communities, I believe it is a tool worth wielding—wisely, collaboratively, and with a shared objective of taking out the economic incentive to commit crime.

David Tyree, Asset Forfeiture Law and Former Special Agent with the DEA, US

TARGETED FINANCIAL SANCTIONS IN THE EU AML/CTF FRAMEWORK: FROM POLICY TO PRACTICE

Georgios Pavlidis

Targeted financial sanctions (TFS) have long been a tool for disrupting terrorism financing and the proliferation of weapons of mass destruction. In the European Union (EU), they have evolved into a broader instrument for upholding international law, safeguarding human rights, and addressing geo-political crises. Their growing integration into the EU's anti-money laundering and counter-terrorism financing (AML/CFT) framework marks a significant shift towards using financial integrity mechanisms to enforce sanctions more effectively. Two recent EU legislative acts – *Directive (EU) 2024/1640* (*Sixth AML Directive, AMLD6*) and *Regulation (EU) 2024/1624* (*AML Regulation, AMLR)* – embed TFS into the AML/CFT architecture. This integration is designed not only to meet the EU's international obligations, but also to close the operational and organisational gaps that have previously allowed sanctions to be circumvented.

A Clearer Legal Foundation

The *AMLR* now offers a precise definition of TFS, covering both asset freezes and prohibitions on making funds or other assets available – directly or indirectly – to designated persons or entities (Article 2(1)(49) *AMLR*). The legal basis for designations rests on a two-tier system: Council decisions taken under the EU's Common Foreign and Security Policy (Article 29 TEU) and Council Regulations as binding financial restrictions implemented under Article 215 TFEU. This framework ensures uniform application across all Member States, giving TFS measures both political legitimacy and enforceable legal effect. By linking sanctions policy to AML/CFT enforcement structures, the EU aims to detect and prevent circumvention more effectively – an increasingly complex task as illicit financial flows adapt to sanctions regimes.

Risk Assessments and Data-Driven Oversight

One of the most notable innovations in *AMLD6* is the explicit requirement to integrate TFS into both supranational and national risk assessments. The European Commission, working with the new Anti-Money Laundering Authority (AMLA), must now assess not only money laundering and terrorism financing threats, but also the risks associated with non-implementation or evasion of TFS in the context of the supranational risk assessments. At the national level, Member States must factor TFS into their own national risk assessments and ensure that preventive measures are tailored accordingly. This risk-based approach aligns with Financial Action Task Force (FATF) principles, but applies them specifically to sanctions compliance. Complementing this, Article 9(2)(k) AMLD6 introduces mandatory statistical monitoring of TFS enforcement – including the value of assets frozen, transactions blocked, and resources allocated to enforcement bodies. These data requirements will help identify gaps, measure impact, and adjust strategies over time.

Strengthened Roles for Public Authorities

TFS compliance is not left solely to the private sector. *AMLD6* expands the responsibilities of key public bodies. Central registers of beneficial ownership in EU Member States must screen their data against sanctions lists, both upon designation and periodically. This helps uncover attempts to hide sanctioned interests behind complex ownership structures. For their part, Financial Intelligence Units (FIUs) in EU Member States gain direct access to detailed information on frozen funds and assets, improving their ability to detect patterns of evasion. Finally, supervisory authorities in EU Member States are tasked with auditing obliged entities' TFS controls, ensuring that internal policies are fit for purpose and that the latest sanctions lists are disseminated promptly. In the same context, the creation of AMLA adds an EU-level supervisory and coordination layer, with a mandate to guide national authorities, promote consistent enforcement, and analyse cross-border evasion risks.

New Compliance Expectations for Obliged Entities

Financial institutions, designated non-financial businesses and professions, and other obliged entities in EU Member States now face clearer and more stringent duties around TFS. These include: a) incorporating TFS risks into business-wide risk assessments and internal controls; b) screening customers and beneficial owners against sanctions lists before onboarding and on an ongoing basis; c) immediately freezing assets and reporting to authorities where a match is found; d) excluding simplified customer due diligence where there is a suspicion of sanctions circumvention. Compliance officers play a pivotal role in ensuring these obligations are met – from calibrating screening tools to liaising with FIUs and supervisors. Given the complexity and speed of sanctions updates, investing in technology and training is essential.

Implementation Challenges

Despite the strengthened framework, several obstacles remain. First, enforcement standards and resources vary between EU Member States, creating uneven implementation and potential safe havens. Second, the use of shell companies, nominee arrangements, and – increasingly – virtual assets complicate detection. Decentralised finance (DeFi) platforms and privacy-enhancing technologies present further challenges. Third, delayed or limited cross-border data sharing, and insufficient guidance can undermine timely action. Addressing these issues at EU level will require political commitment, robust supervisory cooperation, and investment in advanced analytics – including AI-driven monitoring and blockchain forensics.

Looking Ahead

The integration of TFS into the EU AML/CFT framework reflects a broader trend: sanctions enforcement is no longer confined to foreign policy circles but is becoming an operational priority for financial integrity regimes. As geopolitical tensions, human rights concerns, and transnational crime continue to drive sanctions policy, the EU's approach could influence other jurisdictions seeking to link sanctions compliance to AML/CTF supervision. However, legislative reform alone will not guarantee success. Effectiveness will depend on the capacity of both public and private actors to adapt, cooperate, and innovate in response to rapidly changing risks. The next few years will test whether the EU's enhanced framework, which includes the AMLD6 and AMLR, can deliver on its promise: safeguarding the integrity of the EU financial system while reinforcing the credibility of its sanctions policy.

Dr Gergios Pavlidis, Associate Professor - Neapolis University Pafos, Cyprus, UNESCO Chair and Director of the Jean Monnet Centre of Excellence AI-2-TRACE-CRIME.

BEYOND THE STABLECOIN SCARE: SANCTIONS EVASION'S BIGGER PICTURE

Kristofer Doucette

Stablecoins now move trillions of dollars a year, bypassing the very banking infrastructure that sanctions depend on to bite. For sanctioned actors, they create a direct lane to shift dollar assets instantly, outside of chokepoints like SWIFT or correspondent banks. Yet the same rails that worry regulators are quietly reshaping daily life for others. Across Asia and the Pacific, migrant workers are using stablecoins to send money home in minutes for a fraction of the 6–8% fees charged by traditional services. In corridors linked to Australia, where Pacific Island economies rely heavily on remittances, this utility is hard to ignore. The challenge for policymakers is fostering that innovation while guarding against its exploitation by sanctioned regimes.

Stablecoins Under the Spotlight

The case of stabelcoin 'A7A5' shows what happens when the balance tilts the other way. This ruble-backed network, tied to Russian state actors, built a parallel payment channel designed to sidestep enforcement. Sanctions work precisely because transactions must pass through regulated intermediaries; when blockchain rails cut around that architecture, those controls are blunted.

> And that is the larger point: the real danger is not stablecoins in isolation. They become most problematic when woven into the older playbook—shell companies, opaque banking ties, and trade misinvoicing—that states and criminal networks have long used to move value in the shadows.

Old Tricks Enhanced By New Tools

Sanctions evasion has never been static. Whenever restrictions tighten, determined actors adapt. Historically, most evasion schemes have relied on familiar practices: cash couriers, shell companies, fraudulent trade documentation, or complicit facilitators in banking and business. Today, what stands out is not the replacement of these methods, but the way cryptocurrency is integrated into them, amplifying their efficiency and scale.

Operation Destabilise, a major international investigation launched in the United Kingdom in 2021, exemplifies this hybrid approach. The operation targeted Russian laundering networks that blended proceeds from drug trafficking, ransomware, espionage, and sanctions violations. While cryptocurrency featured prominently—particularly through exchanges such as Garantex—the operational backbone remained fundamentally low-tech: cash couriers transporting millions across Europe. However, once consolidated, these proceeds could be converted into stablecoins, creating a synthesis of conventional smuggling operations with digital asset capabilities that significantly complicated detection and interdiction efforts. The estimated value laundered through these channels exceeded $700 million.

Similarly, in 2023, the Australian Federal Police, in coordination with international partners, dismantled a sprawling Chinese-run money laundering network operating through the Changjiang Currency Exchange. The scheme presented as a classic cash-intensive remittance operation, maintaining physical storefronts across multiple Australian cities. Between 2020 and 2023, nearly AU$229 million was processed through the network. Behind the counters, however, operators layered transactions into cryptocurrency wallets, introducing additional obfuscation to already murky financial flows. This case demonstrated how manual cash handling processes continue to represent operational vulnerabilities, while cryptocurrency integration serves as a technological force multiplier for laundering operations.

North Korea's record shows that sophisticated sanctions evasion long predates the advent of cryptocurrency. Pyongyang has smuggled coal and weapons by sea, printed counterfeit US currency, trafficked methamphetamine, and engineered one of the most infamous bank heists of the digital era: the 2016 theft from Bangladesh's central bank via the SWIFT network. These operations illustrate how North Korea has mastered sanctions evasion as an art form, relying on front companies and covert finance networks. While crypto has since been added to this arsenal, it is just one tool among many. The regime's capabilities remind us that new technologies can accelerate, but are not required for sanctions evasion to thrive.

The pattern across these cases is clear: stablecoins are rarely the center of gravity. Rather, they are integrated into established networks that already demonstrate operational resilience and strategic sophistication.

The Pitfalls of Tunnel Vision

The distinction carries significant policy implications, as policy debates too often fall prey to tunnel vision. The growth of stablecoins has captured political attention, creating risk that these instruments will become perceived as the primary battleground for sanctions enforcement effectiveness. The resulting policy temptation is to equate comprehensive stablecoin regulation with closing sanctions vulnerabilities. This approach risks implementing targeted solutions for secondary channels while leaving primary vulnerabilities unaddressed.

Such analytical tunnel vision produces several dangers. Policymakers may craft rules that choke off stablecoin issuers while overlooking more established conduits, such as trade-based laundering, real estate investment, or the use of lawyers' trust accounts. Additionally, this approach reinforces the misconception that technology itself is the enemy. Sanctions evaders demonstrate no allegiance to cryptocurrency; they are opportunists who migrate toward the most accessible operational pathway.

Casting a Wider Net on Illicit Finance

Some governments are beginning to broaden their regulatory approach. In Australia, the passage of long-delayed 'Tranche 2' reforms in 2024 represented a fundamental shift. For the first time, lawyers, accountants, real estate agents, and company formation providers will be brought under anti-money laundering and counter-terrorist financing obligations. By 2026, roughly 90,000 new entities will face compliance requirements.

This expansion matters for sanctions enforcement because illicit money does not flow in isolation. It moves through property purchases, opaque corporate structures, and professional intermediaries. Australia's own assessments had flagged lawyers as a 'high and stable' money laundering vulnerability. Until this regulatory expansion, however, they operated largely outside regulatory scrutiny. By plugging these gaps, Australia is strengthening the overall financial system, rather than chasing only the latest tool.

The United States is moving in the same direction. The GENIUS Act of 2025 created the first comprehensive federal framework for payment stablecoins. Issuers and exchanges must now maintain appropriate licenses, back issued tokens with adequate reserves, and implement sanctions screening protocols. While it doesn't fully solve the problem, it brings digital asset providers into the compliance perimeter and narrows the loopholes, representing meaningful progress toward systematic change.

Beyond the Tech: The Human Factor

Policy debate must move beyond the assumption that technology itself is the villain. Blockchain protocols cannot launder money without human actors directing the flows. Sanctions evasion consistently requires human facilitators—lawyers who set up offshore structures, over-the-counter brokers who turn a blind eye, bankers who grease the wheels. Stablecoins are merely tools the actors employ.

Recognising this reality means focusing enforcement efforts on facilitator networks, not just the instruments they use. Cracking down on issuers without addressing complicit professionals risks, leaving the system vulnerable.

A Balanced Strategy for an Old Crime

Sanctions evasion is, at its core, an old game. Stablecoins are simply the latest mousehole for evaders to slip through, but they are not the only one. Winning requires covering all the holes at once, rather than boarding up whichever one happens to be in the headlines. This approach necessitates intelligent stablecoin regulation that keeps them inside compliance frameworks. It also means reinforcing the less glamorous parts of the system—shell companies, real estate, trade finance, and professional gatekeepers—where illicit finance has thrived for decades. Above all, it means understanding that sanctions evasion is driven by adaptive human networks, not by any single technology.

The right approach is balance. Stablecoins must remain part of the regulatory discussion, but never the whole discussion. Only by seeing the bigger picture can policymakers hope to blunt the resilience of adversaries who have been evading sanctions long before crypto existed—and who will continue adapting long after the headlines have moved on.

Kristofer Doucette, President of Applied Technology Solutions, Former Director of National Security Solutions - Chainalysis Inc., Former Senior Analyst - US Dept of the Treasury.

TARGETED FINANCIAL SANCTIONS: A CALL FOR ACCOUNTABILITY AND REFORM IN GLOBAL COMPLIANCE

Sisira Dharmasri Jayasekara

Targeted financial sanctions (TFS) have emerged as a critical tool in the global effort to main peace, combat terrorism, and improve the quality of life for people around the world. These sanctions are designed to restrict access to financial systems for individuals, entities, and regimes involved in terrorism financing, money laundering, and the proliferation of weapons of mass destruction. However, the implementation and consequences of these sanctions, particularly in jurisdictions under increased monitoring by the Financial Action Task Force (FATF), raise important questions about fairness, accountability, and effectiveness.

A recurring challenge among countries placed under FATF's increased monitoring, often referred to as the "grey list", is the lack of a robust legal and institutional framework to effectively implement TFS. These jurisdictions, many of which are emerging economies, face a host of macroeconomic difficulties that already strain the living standards of their populations. The deficiencies identified by FATF are typically not due to active support for terrorism, but rather the failure to establish and enforce mechanisms that prevent the misuse of financial systems for illicit purposes. The responsibility for creating and maintaining an effective sanctions regime lies squarely with the government and its designated institutions. These entities are entrusted with the authority and resources to ensure compliance with international standards. However, when they fail to fulfil this mandate, the consequences often fall not on the officials responsible, but on the general population.

Sanctions imposed on a country as a whole can lead to economic isolation, increased transaction costs, and reduced access to international financial systems—all of which disproportionately affect ordinary citizens.

In democratic societies, the government acts as an agent of the people, who are the principal stakeholders. Citizens delegate authority to public officials with the expectation that they will act in the public interest and uphold both domestic and international obligations. When these agents fail in their duties, whether through negligence, incompetence, or lack of political will—they breach the trust placed in them by the public. Under the principles of agency law, such breaches can give rise to legal remedies, including claims for damages and other forms of accountability.

This concept of agency is particularly relevant in the context of FATF compliance. If a government or its institutions fail to implement effective measures to counter terrorism financing, the blame should not be placed on the country's population. Instead, targeted accountability should be directed at the specific officials and agencies responsible for the failure. Unfortunately, current sanctioning mechanisms often overlook this distinction, resulting in collective punishment that undermines the very goals of the global anti-money laundering and counter-terrorism financing (AML/CFT) framework.

Mutual evaluation reports conducted by FATF and its regional bodies provide a detailed assessment of a country's compliance with international standards. These evaluations examine the effectiveness of measures to combat money laundering, terrorism financing, and the financing of weapons proliferation. A common pattern observed in these reports is that many emerging economies are repeatedly placed under increased monitoring following each evaluation cycle. This suggests a persistent lack of commitment or capacity among the responsible authorities to address identified shortcomings.

The consequences of being grey-listed are significant. Financial institutions in other countries may impose enhanced due diligence measures on transactions involving the listed jurisdiction. This can lead to increased costs for businesses and consumers, delays in cross-border payments, and restrictions on access to international banking services. In some cases, countries may face additional countermeasures, such as limitations on correspondent banking relationships or restrictions on trade. These outcomes can severely impact economic growth and development, further exacerbating poverty and inequality.

Ironically, the people who suffer the most from these consequences are those who had no role in the failures that led to the sanctions. Meanwhile, the officials and institutions responsible often face little to no accountability. In many emerging economies, public officials enjoy significant privileges, including frequent international travel and limited oversight. The principle of institutional independence, while important for ensuring impartiality, is sometimes misused to shield officials from scrutiny and responsibility. Given that FATF has been conducting mutual evaluations since its establishment in 1989, the recurring nature of non-compliance in certain jurisdictions raises questions about the effectiveness of the current approach. If the same countries continue to fall short of expectations despite repeated evaluations and technical assistance, it may be time to reconsider the strategy.

Rather than imposing broad sanctions that harm entire populations, global policymakers should explore alternative measures that focus on holding specific public authorities and officials accountable.

One potential avenue for reform is the promotion of public interest litigation. Citizens, civil society organisations, and advocacy groups could initiate legal action against government officials and agencies that fail to implement effective AML/CFT measures. Such litigation would not only promote accountability but also raise public awareness about the importance of financial integrity and the consequences of non-compliance. It would also reinforce the principle that public officials are answerable to the people they serve.

Furthermore, international organisations and donor agencies could play a more active role in supporting institutional reform. This could include capacity-building programs, technical assistance, and the development of accountability frameworks that ensure responsible governance. By focusing on systemic improvement and individual accountability, the international community can help countries build resilient institutions that are capable of meeting global standards, without punishing their citizens for the failures of their leaders.

While TFS are a vital tool in the fight against terrorism and financial crime, their implementation must be guided by principles of fairness, accountability, and effectiveness. The current practice of imposing broad sanctions on entire jurisdictions often results in unintended harm to innocent populations, while allowing the true culprits—ineffective or negligent public officials—to escape responsibility. A more just and effective approach would involve holding these officials accountable, promoting institutional reform, and ensuring that the burden of compliance does not fall on those least able to bear it. Only then can the global AML/CFT framework achieve its intended goals of security, stability, and prosperity for all.

Sisira Dharmasri Jayasekara, Additional Chief Accountant at The Central Bank of Sri Lanka, Finance Department.

TARGETED FINANCIAL SANCTIONS: EFFECTIVENESS, CHALLENGES AND UNINTENDED CONSEQUENCES

Dare Joseph Ayinde

The imposition of financial sanctions on specified individuals and entities with a view to coercing them into abandoning their involvement in activities that threaten global peace and the integrity of the international financial system has been on the increase in the past two decades. The sanctions, which mainly involve the freezing and prohibition of the transfer of funds and assets to and from the designated individuals and entities, are designed to cripple the capacity of the designated individual and entities to finance State-backed or group's criminal activities. In addition, they are geared towards preventing rogue States and entities from exploiting the international financial system to further their obnoxious activities.

In contrast to broad-based sanctions, targeted financial sanctions seek to exert the maximum pressure on individuals and entities that control or play key roles in the activities of groups or States that are complicit in terrorism and terrorist financing, and the proliferation of weapons of mass destructions with limited negative externalities. The obligation to impose these sanctions stems from the United Nations Security Council Resolutions for the involvement of an individual or a group in terrorism and terrorist financing. In addition, Article 8 of the International Convention for the Suppression of the Financing of Terrorism, and Recommendations 6 and 7 of the Finance Action Taskforce Standards obligate States to impose targeted financial sanctions on individuals and entities that are involved in terrorism and terrorist financing, and the proliferation of weapons of mass destructions. Apart from these, supra-national organisations, such as the European Union, and some States, such as the United States of America and the United Kingdom, also use targeted financial sanctions as economic statecraft.

Unlike other forms of targeted sanctions such as travel ban and arms embargo, the imposition of targeted financial sanctions on designated individuals and entities often lead to dire economic consequences for the targeted State. Studies have shown that the imposition of financial sanctions on some Russian Banks and entities have restricted them from global financial system and cross-border trades and transactions.

Similarly, the imposition of financial sanctions on designated individuals and entities in Iran has greatly impacted on its economy negatively. Specifically, it has led to a significant decrease in its export and oil production, and led to an increase in inflation. Although these sanctions, to a great extent, have been effective in restricting the access of the sanctioned individuals and entities to the global financial system, its effectiveness in compelling the targeted State to change its policies is in doubt. For example, despite the different forms of targeted financial sanctions that have been imposed on designated individuals and entities in Russia, following its annexation of Crimea and the subsequent invasion of Ukraine, there has not been any significant change in Russia's policy in its aggression against Ukraine.

Challenges:
One major challenge to the effectiveness of targeted financial sanctions is the use of alternative payment platforms, such as cryptocurrency, by targeted individuals, entities and States to evade the sanctions. Studies show that there has been a significant increase in the use of cryptocurrency and other virtual currencies in sanctioned jurisdictions, such as Russia, Iran and North Korea, which have been linked to efforts to circumvent the sanctions imposed on designated individuals and entities in these States. In 2024, targeted States and sanctioned entities purportedly received 15.8 billion United State dollars in cryptocurrency, and this constituted 39 per cent of crime-related crypto transactions. Sanctioned individual, entities and States resort to these platforms because they are inadequately regulated.

Consequently, through the use of cryptocurrency, individuals and entities that are subject to sanctions are able to engage in cross-border business trade, thereby circumventing the restrictions imposed on them from using the global financial system. In a bid to counter the use of cryptocurrency, and other virtual currencies in evading sanctions, the United State through the Department of Treasury's Office of Foreign Assets Control has imposed sanctions on cryptocurrency exchange platforms which are complicit in sanctions evasion, seized their internet domain names and froze their assets but the problem still persists.

One reason targeted financial sanctions is preferred over broad-based sanctions is that it has limited effects on vulnerable groups and innocent citizens, unlike broad-based sanctions.

Unintended Consequences:
Nonetheless, it has some unintended consequences. One such unintended consequences is that they sometimes lead to collateral damage. This may happen where targeted financial sanctions are imposed on several individuals and entities or major actors in an important sector of the economy. The imposition of targeted financial sanctions on such individuals and actors could cripple the sector. Thus, the impacts of the sanctions would not only be felt by those targeted by the sanctions but also by the innocent players in the sector and the citizens, and this may lead to severe humanitarian consequences.

Another unintended consequence of targeted financial sanctions is de-risking. In a bid to avoid inadvertently engaging in business transactions with individuals and entities that are subject to financial sanctions, financial institutions sometimes avoid all transactions that relate to the targeted States. This hampers the capacity of humanitarian organisations to promptly address humanitarian needs and emergencies. Similarly, targeted financial sanctions could lead to overcompliance by financial institutions. It has been reported that some financial institutions, for example in relation to Syria, have been unduly stringent in processing payments relating to transactions involving the targeted State for the fear that the funds would be redirected to sanctioned individuals and entities.

As a result of these, humanitarian organisations do have difficulties in paying their staff and providing funds to carry out their humanitarian work. In order to mitigate the harshness of financial sanctions on innocent civilian populations, essential humanitarian aid items, such as food and medicine, are often exempted from the scope of the sanctions. However, the multilayer bureaucratic processes of obtaining approval for the processing of financial transactions relating to these items are sometimes cumbersome, thus undermining the timely delivery of humanitarian aid items.

Notwithstanding the seeming ineffectiveness and the unintended consequences of targeted financial sanctions, they are still very much useful in pressuring States and groups to abandon activities that undermine the integrity of the global financial system and stability. However, there is a need for the sender State to continuously appraise the effectiveness of financial sanctions that are imposed on designated individuals and entities, and respond with appropriate measures to counter steps that the targeted State takes to evade or weaken the effectiveness of the sanctions. Also, practical measures should be taken to ensure that targeted financial sanctions have minimal humanitarian consequences.

Dr Dare Joseph Ayinde, Lecturer Faculty of Law of Ajayi Crowther University, Nigeria.

REGULATORY SANCTIONS FOR AML/CTF NON-COMPLIANCE: BACKGROUND CASE

William Gaviyau

GHY Bank Ltd is a commercial bank with presence in three continents namely Asia, Europe and Africa. Donnel Alie, the Chief Compliance Officer of GHY Bank Ltd, is a highly qualied and experienced officer with anti-money laundering and counter-terrorism financing (AML/CFT) related qualifications. He was responsible for ensuring compliance with AML/CFT regulations for the bank. Despite his role, Donnel failed to adequately perform his duties, leading to significant AML/CFT non-compliance issues resulting in severe regulatory sanctions imposed against both the Chief Compliance Officer and GHY Bank Ltd. The following case points out the regulatory sanctions that can be imposed by regulators for non-compliance.

Key Issues Raised by the Case of GHY Bank Ltd

The key issues raised by the case include, firstly, that the case highlights poor internal control procedures, inadequate reporting mechanisms and inadequate staff training. This case emphasizes the importance of companies' internal AML/CTF controls to mitigate financial crime risk and maintain the integrity of the financial system. Secondly, the case demonstrates a failure to comply with regulatory, institutional, operational and legal risks. Every decision within the organisation points to accountability. Thus, regulatory officers and financial institutions must be held accountable for their actions, and failure to comply with regulations can result in severe consequences. Thirdly, the case highlights that ways to mitigate the risks of non-compliance include staff training and education, and improved internal controls. Adequate training and education are crucial for regulatory officers and staff to ensure compliance with AML/CFT regulations. However, education and experience does not guarantee compliance; rather, risk compliance entails a continuous learning process as the operating environment evolves.

The case of GHY Bank Ltd highlights the urge by regulators to continually concertise stakeholders on the importance of AML/CFT regulations and implications of non-compliance. Each country's AML/CFT regulations are derived from the Financial Action Task Force (FATF)'s recommendations. These recommendations provide a framework of measures to combat money laundering and financing of terrorism.

Regulatory Enforcement Mechanisms

Enforcement actions directed at financial institutions and designated non-financial institutions are imposed to ensure that AML/CFT compliance frameworks are consistent and upgraded in line with legislative requirements. Additionally, enforcements denote failures in operational programs and processes. There are three regulatory enforcements, namely cease and desist orders; forfeiture orders; and monetary penalties.

Cease and Desist Orders

The 'cease and desist order' is issued when a financial institution or designated non-financial institution fails to establish and maintain an appropriate AML/CFT program or correct previously identified regulatory deficiencies. Accordingly, this order is issued under these two circumstances which can be concurrent. Firstly, failure to maintain the established AML/CFT program. For example, AUSTRAC issued remedial action notice to Australian Military Bank Ltd in 2021 for failure to conduct a money laundering and terrorism financing risk assessment and inadequate related systems, controls, and documentation. Secondly, failure to rectify AML/CFT regulatory deficiencies previously identified. An example of this is when the Office of Comptroller Currency of USA issued a cease-and-desist order against Bank of America in 2024 for failure to timely file suspicious activity reports and correct a previously identified deficiency related to its customer due diligence processes.

Financial Penalties

Financial penalties are levied on repetitive legal infringements or failure to effect corrective measures. To illustrate, in 2020, State Street Bank and Trust Company was issued with a penalty amounting to A$1.247 million for failure to abide by the AML/CFT provisions by AUSTRAC. Also, the South African Reserve Bank (SARB) imposed administrative sanctions on Old Mutual Life Assurance Company for non-compliance with the Financial Intelligence Centre Act (FICA) in 2024. The regulatory sanction was a financial penalty totalling ZAR15.9 million. The regulatory authorities are also obliged to institute personal liability. For example, in 2014, Financial Crimes Enforcement Network (FinCEN) of USA issued a civil monetary penalty to MoneyGram's Chief Compliance Officer amounting to USD1 million. This was for failure to ensure MoneyGram abided by the AML/CFT provisions of Bank Secrecy Act over a long period of time. Also, the 2018`s Rabobank of USA case, an employee was demoted, or contract terminated for failure to raise query on the transaction with the authorities on the inadequacy of the AML/CFT program. The bank was eventually fined USD360 million on the related AML/CFT weaknesses.

Forfeiture Orders

The 'forfeiture order' is issued as a last resort after exhausting all the other remedies. This order entails removing the assets from the institution`s operations. Most countries have this provision in their legislation. However, to date, no regulator has exercised this order. This might indicate that regulators fear exercising this order as this could cause financial instability in the economy. If instituted, this goes against the regulator's mandate of maintaining financial stability and consumer protection among others.

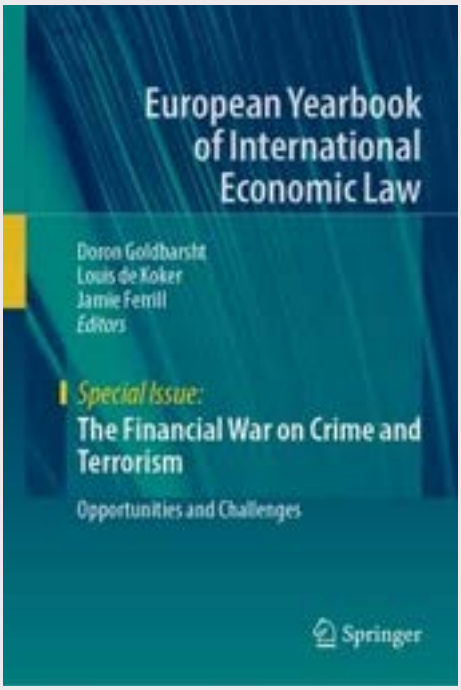
Conclusion

Enforcement of AML/CFT regulations remain beneficial in the long run, though in the short run it cannot be understood. Hence, effective compliance with AML/CFT regulations plays a crucial role in maintaining the integrity of the financial system and mitigating financial crimes incidences. By prioritising compliance and taking a proactive approach to AML/CFT regulations, financial institutions and designated non-financial institutions can reduce the risk of non-compliance, contributing to financial stability and financial integrity.

Dr William Gaviyau, Post Doc Fellow, University of South Africa, Department of Finance, Risk Management & Banking.

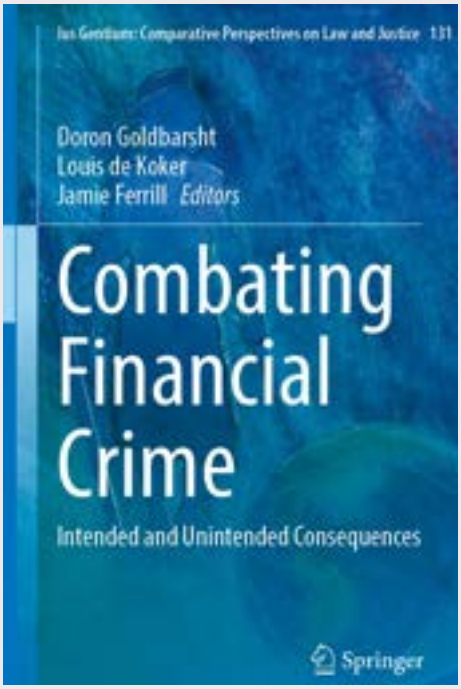
RESEARCH AT FIH

THE FINANCIAL WAR ON CRIME AND TERRORISM: OPPORTUNITIES AND CHALLENGES (FORTHCOMING 2025)



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-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.

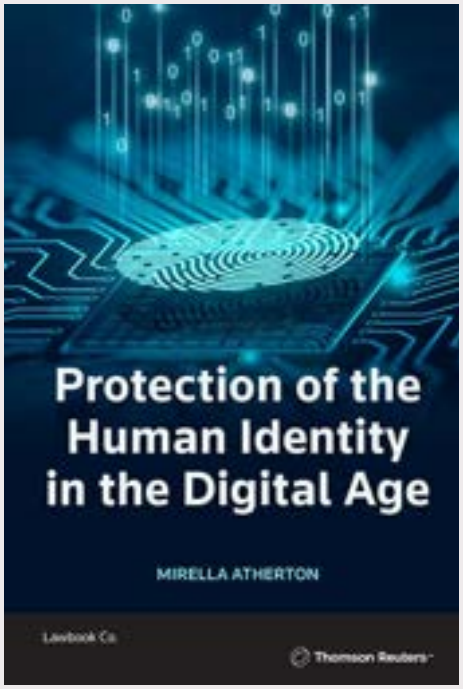
COMBATING FINANCIAL CRIME: INTENDED AND UNINTENDED CONSEQUENCES (FORTHCOMING 2025)



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

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



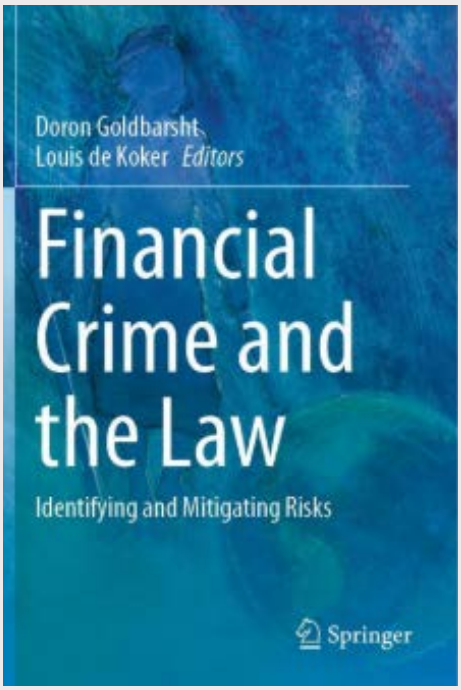
Written by Mirella Atherton, this book examines how digitalisation, artificial intelligence, big data, and global connectivity are reshaping concepts of privacy, autonomy, and security. The book examines how human identity and mass data collection intersect. It begins with a theoretical insight into 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.

AUSTRALIA'S FINANCIAL INTEGRITY: A GLOBAL COMPLIANCE APPROACH TO AML/CTF (2024)

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.

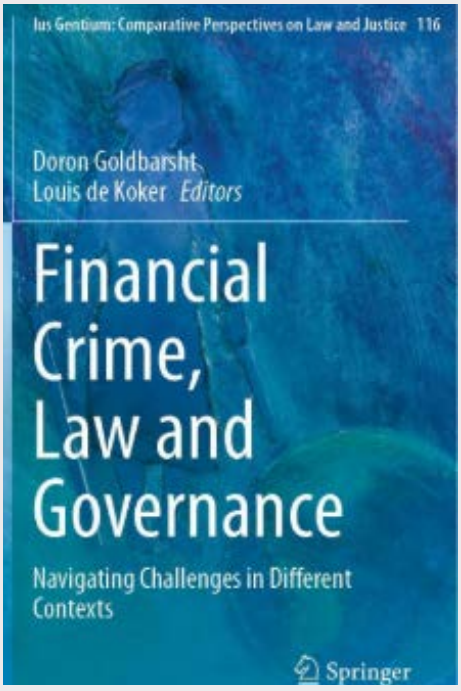
RESEARCH AT FIH

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



Edited by Doron Goldbarsht and Louis De Koker, this collection explores financial crimes like crypto crime, terrorist financing, and money laundering. It offers insights into risk-based compliance, challenges in regulating weapons of mass destruction financing, and the connection between cannabis regulation and money laundering. The book also critiques the effectiveness of the risk-based approach, highlighting concerns about bias and the role of 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)



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

FIH PODCAST

Listen to us on Spotify!

Season 2 of the *Financial Integrity Hub Podcast*

The Financial Integrity Hub hosts regular podcasts, 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 - Perspectives on AML/CTF with Dr Rachel Southworth, Prof Michael Levi, Prof Louis De Koker, and Charles Littrell.

Episode 2 - Risk Management in Casinos with Armina Antoniou

Episode 3 - Financial & Environmental Crime with Davyth Stewart

Episode 4 - The AML/CTF Act and the Reform with Jeremy Moller

Episode 5 - Meet the CEO: In Conversation with Brendan Thomas

Episode 6 - Disrupting Terrorist Financing: A Conversation with Dr Matthew Levitt

NEW! Episode 7- Financial Crime and Current Challenges, with Jason Sharman
Dr Hannah Harris speaks with financial crime expert, Jason Sharman, to explore threats facing the global financial system—from money laundering and sanctions, to emerging risks in digital finance.

Thank you to our podcast partner - CFCE!

CFCE sets itself apart as an exceptional AML/CTF training provider with a unique focus on the Australian industry.

CFCE
CERTIFIED FINANCIAL CRIME EXPERTS

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

3 UNDER 30 EVENT

DRIVING THE FUTURE OF FINANCIAL INTEGRITY

Date: 25 September 2025, Thursday
Time: 6:30pm-8pm
Location: Tank Stream Bar, Establishment Precinct – 1 Tankstream Way, Sydney NSW 2000

Join us as we spotlight the next generation of leaders shaping the fight against financial crime. This event brings together three outstanding professionals under 30 from industry, government, and academia, rising stars already making their mark.

Hear their stories, insights, and vision for the future of financial integrity. Walk away with practical advice, fresh perspectives, and inspiration, plus the chance to connect with leaders across the AML/CTF community. Proudly supported by FIH, AUSTRAC and Hamilton Locke.

For tickets, please visit the FIH Website or scan the QR Code.

END OF YEAR EVENT

HARNESSING TECHNOLOGY FOR FINANCIAL INTEGRITY

11 December 2025, Thursday

From machine-learning and artificial intelligence to advanced analytics, technology is reshaping how regulators, regulated entities, and enforcement agencies detect and prevent financial crime. As the sector faces growing complexity and regulatory demands, this event offers key insights into the future of AML/CTF regulation and the technologies shaping it.

Bringing together experts from industry, government, and academia, this event will examine the opportunities and challenges of leveraging technology to strengthen financial integrity.

For tickets, please visit the FIH Website.

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