June Issue 2026

FIH INSIGHTS

Making AML Compliance Work for Small Business

Following the Money Behind Organised Crime

From Grey-Listed to Gatekeeper

Regulating the Gatekeepers

TANIA WOLFF

ISSN: 2982-3188

LEADERSHIP

Patron
Hon. Patricia Bergin AO SC

Director
Associate Professor Doron Goldbarsht

Associate Director
Isabelle Nicolas

Advisory Board
Armina Antoniou
Joanna Bird
Professor Louis De Koker
Paul Jevtovic APM OAM
Professor Elizabeth Sheedy
Michael Tooma
Stuart Clark AM (d. June 2025)

Reference Group
Sue Bradford
Gail Carter
Claudine Lamond
Jeremy Moller

Research Fellows
Professor Sean Foley
Dr Mirella Atherton
Dr Daley Birkett
Dr Derwent Coshott
Dr Jamie Ferrill
Dr Hannah Harris
Dr Jeanne Nel

Researchers
Shehnila Iqbal
Giang Nguyen
Isabelle Nicolas
Samuel Orchard
Ben Scott

Interns
Reem Armanno (Editor)
Lucienne Champion
Luke Gabriel
Ella Garling

Citing reference: Financial Integrity Hub 'FIH Insights' (2026) 3(2) FIH, Sydney
<https://www.mq.edu.au/research/research-centres-groups-and-facilities/groups/financial-integrity-hub/engagement>.

Featured on the cover, President, Law Council of Australia, Tania Wolff.

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:

FINANCIAL INTEGRITY HUB

MACQUARIE University SYDNEY·AUSTRALIA

TABLE OF CONTENTS

- **Regulating the 'Gatekeepers': A Global Turning Point in AML/CTF Supervision**
- **Opinion Pieces**
  - Interview with Tania Wolff
    President, Law Council of Australia
  - From Obligation to Action: Making AML Compliance Work for Small Business
    Daniel Mossop and Alex York
  - Trusted Legal Adviser and Gatekeeper: Balancing Client Experience and AML/CTF Obligations
    Carol Prasad
  - Tipping the Wink: What Disclosures Offend s 123 AML/CTF Act?
    Mathew Leighton-Daly
  - Moving Professions From Grief to Acceptance in the AML/CTF Journey
    Alice Saveneh-Murray
  - Constructing Compliance as Legal Culture: Assessing the Potential for More Effectiveness
    Go Lisanawati
  - Regulating the Gatekeepers: Following the Money Behind Organised Crime
    Katie Bourne and Huey Lam
  - When Compliance Looks Right but Fails: The Real Risk Behind Tranche 2 Reform
    John Kouroutzoglou
  - Making the New EU AML Authority Count: Three Tests
    Sunny Nagpal
  - From Grey-Listed to Gatekeeper: Regulating Professional Service Providers as AML/CTF Frontline Actors (Lessons from South Africa)
    Abraham Ename Minko
  - Gatekeepers Without Visibility: Structural Limits on DNFBPs in Detecting Financial Crime
    Nazim Khaja

- **FIH Research**
- **FIH Podcast**
- **FIH Events**
- **FIH Insights Previous Editions**

REGULATING THE 'GATEKEEPERS'

A GLOBAL TURNING POINT IN AML/CTF SUPERVISION

Image: Dr Katie Benson, Katie Miller, Neil Jeans, Isabelle Nicolas at the 2026 *Financial Integrity Week* DNFBP Panel.

Reem Armanno | Editor

For decades, anti-money laundering and counter-terrorism financing (AML/CTF) regulation has focused primarily on banks and other financial institutions. Around the world, regulators are increasingly recognising that the fight against financial crime cannot be won by the financial sector alone. The professionals who facilitate business formation, property transactions, asset management, and complex financial arrangements have become a critical part of the global AML/CTF framework.

This shift reflects a growing reality: sophisticated financial crime rarely occurs in isolation. Criminal networks increasingly rely on professional expertise to establish corporate structures, move funds, acquire assets, and obscure beneficial ownership. Lawyers, accountants, real estate professionals, trust and company service providers, and dealers in precious metals and stones occupy positions of trust within the legitimate economy. While the overwhelming majority operate with integrity, their services can also be exploited by those seeking to disguise the proceeds of crime or conceal illicit activity.

As a result, jurisdictions across the globe are extending AML/CTF obligations beyond traditional reporting entities to encompass these so-called "gatekeeper" professions. What was once viewed as a niche regulatory issue has become one of the most significant developments in financial crime prevention policy. Yet the debate is about more than compliance. It raises fundamental questions about where responsibility for safeguarding the financial system should lie. To what extent should private professionals be expected to detect and disrupt illicit activity? How can governments strengthen financial integrity without undermining professional independence, confidentiality, and trust?

This edition of *FIH Insights* explores the international movement to regulate designated non-financial businesses and professions (DNFBPs) within AML/CTF frameworks. By examining global trends, implementation challenges, and lessons from jurisdictions that have already travelled this path, we aim to provide practical insights for Australia as it enters a new era of gatekeeper regulation.

Why Gatekeepers Matter

DNFBPs are uniquely positioned: they facilitate corporate formation, manage client assets, structure transactions, and enable high-value purchases. These services are essential to economic activity, but they also create opportunities for misuse. Criminals exploit complex corporate structures, opaque ownership arrangements, and high-value asset transfers to disguise the origins of illicit proceeds.

Real estate transactions, luxury goods purchases, and the creation of shell companies remain among the most common methods for laundering funds globally. These vulnerabilities have downstream impacts on the integrity of financial systems, making the regulation of DNFBPs a necessary complement to traditional financial sector oversight.

The Globlal Regulatory Landscape

Across jurisdictions, approaches to DNFBP regulation vary widely. Some countries have long-standing supervisory frameworks, established reporting obligations, and designated regulators overseeing compliance. Others are only beginning to align domestic systems with the Financial Action Task Force Recommendations—particularly those relating to customer due diligence, suspicious matter reporting, and risk-based compliance obligations for non-financial sectors.

FATF emphasises that DNFBP obligations must be proportionate and risk-based, ensuring that professionals manage money laundering and terrorism financing risks appropriately without imposing unnecessary burdens. For this approach to work, regulators must engage closely with industry to understand operational realities, sector-specific risks, and the practical implications of compliance. This consultation is essential not only to avoid over-regulation, but also to build trust and foster a shared understanding of the role gatekeepers play in safeguarding the financial system.

Australia’s Tranche 2 Reforms: A Pivotal Moment

In Australia, the introduction of the Tranche 2 reforms marks a significant turning point. Bringing DNFBPs within the AML/CTF regime will require the development of new systems, internal controls, and risk management practices. But the implications extend beyond operational adjustments.

Extending AML/CTF frameworks to professional service providers is not without complexity. Many gatekeepers operate within legal and ethical frameworks that emphasise confidentiality, client secrecy, and fiduciary duties. Regulatory systems must therefore be designed to respect these principles while ensuring effective risk mitigation.

Where clients fear that reporting obligations override the trust inherent in professional relationships, the result can be strained interactions, reduced transparency, and unintended consequences for other legal or ethical obligations. Achieving the right balance requires careful legislative design, clear guidance, and ongoing dialogue between regulators and industry.

Jurisdictions with mature DNFBP regulatory systems offer lessons on supervisory models, enforcement strategies, and the practical challenges of extending AML/CTF obligations beyond the financial sector.

Looking Ahead

Ultimately, the success of gatekeeper regulation will not be measured by the number of entities brought within the AML/CTF regime, but by whether those entities are empowered to identify and manage risk in a meaningful and sustainable way. The challenge for regulators is not simply to extend obligations, but to build a framework that is proportionate, practical, and capable of securing industry trust.

As Australia embarks on its Tranche 2 reforms, the opportunity exists not merely to follow international standards, but to help shape what effective gatekeeper supervision looks like in the years ahead.

INTERVIEW WITH TANIA WOLFF

PRESIDENT OF THE LAW COUNCIL OF AUSTRALIA

Could you briefly share your professional journey and what led you to your current role?

My career in the law has not followed a conventional path, and I think that has been its greatest asset. I have worked as in-house counsel, a commercial consultant, a university tutor and lecturer, and a member of both the Victorian Civil and Administrative Tribunal and the Mental Health Tribunal. I have practised in Australia and overseas, including as Legal Counsel with regional responsibility at Aker Kvaerner in Singapore. Each of those roles gave me a different vantage point on how the law operates, and, crucially, where it has challenges.

The experience that defined my practice, though, was the decade I spent building First Step Legal into what it is today. When I joined, it was a nascent service. Over more than 10 years, I drove its expansion into a health justice partnership that embeds integrated legal services directly within health and human service settings—a model that has informed how integrated legal services are delivered across the sector, providing pro bono advice and representation across criminal and family law to people with complex health needs. This model of service delivery—where legal and health professionals collaborate to address the needs of the whole person rather than the presenting problem—was genuinely innovative. Watching it develop and expand gave me both a deep belief in the power of structural reform and a clear-eyed view of where the legal system continues to face challenges.

It was that urgency that led me to join the Board of the Law Institute of Victoria, where I later served as President, and ultimately to the role I hold today. I am proud to be the first President of the Law Council of Australia to have come from the legal assistance sector. It is not a credential I hold lightly—it shapes every conversation I have about what this profession is for.

How do you see the role of legal professionals evolving as part of Australia's anti-money laundering and counter-terrorist financing (AML/CTF) framework, particularly in light of expanding obligations?

The fundamental obligations of lawyers—to the court, their clients, and the administration of justice—have not changed, and the AML/CTF framework does not alter them. What the framework does is formalise and make visible a set of responsibilities that lawyers have always held: know your client, understand the purpose of the transaction, and do not facilitate wrongdoing.

That said, it would be wrong to suggest the new framework changes nothing. It changes the legal and institutional context significantly. For the first time, lawyers providing designated services are formally regulated under the *AML/CTF Act*. That brings external accountability structures, AUSTRAC oversight, and compliance obligations that sit alongside, and must be carefully reconciled with, the profession's existing ethical framework. The challenge is not the substance of what we are being asked to do. The challenge is the architecture: ensuring that how we comply is consistent with who we are as a profession.

What are the key challenges and opportunities for the legal profession arising from expanded AML/CTF regulation?

The most acute challenge we face is the structural tension between the new suspicious matter reporting (SMR) obligation and the tipping-off provision, and what that means for a lawyer's duty to their client. When a lawyer forms a suspicion and lodges a SMR, they are required to terminate the retainer. They cannot tell the client why. That is an extraordinary position to be in. The law is asking lawyers to end a professional relationship in silence, and to do so in circumstances where their client may be entirely unaware they have done anything to give rise to concern.

The Law Council is updating both the *Legal Profession Uniform Legal Practice (Solicitors) Rules 2015* and the *Australian Solicitors Conduct Rules* to navigate this carefully. Retainer agreements will now be required to notify clients upfront that solicitors carry statutory obligations, including reporting obligations, that may require them to terminate a retainer without being able to explain why. We are clarifying that 'just cause' for termination under Rule 13 explicitly covers circumstances where continuing to act would put a solicitor in breach of their ethical or statutory duties. These are not merely technical amendments. They reflect a genuine effort to be transparent with clients about the world lawyers now operate in, while protecting the integrity of the reporting framework.

On the opportunities side, the legal profession is founded on integrity, honesty and commitment to the rule of law. For too long, the legal profession has been characterised, mostly unfairly, as a potential vulnerability in the financial system. The new framework offers an opportunity to change perceptions and demonstrate, credibly and publicly, that lawyers play an active role in safeguarding financial integrity as part of upholding the rule of law.

What practical guidance would you offer to legal professionals preparing to implement new AML/CTF obligations?

The most important 1st step for legal professionals is to determine whether they provide a designated service under s 6 of the *AML/CTF Act*. If they do, they must be ready to comply by 1 July 2026.

AUSTRAC has developed guidance to help practitioners assess whether their services are captured and what their obligations will be. Local Law Societies are also a valuable first point of contact for those with questions. The Law Council is also developing guidance for specific areas of the profession on designated services and more generally about SMR.

The compliance journey involves several interlocking steps: understanding the framework and your specific obligations; enrolling with AUSTRAC; creating an AML/CTF program and policies; appointing a compliance officer; training staff; and integrating the new obligations into everyday practice. Whatever systems and tools you use to do this, the investment of time is not optional. Getting this right requires genuine engagement with the framework, not a tick-box exercise.

One consequence that may surprise smaller practices is that the small business exemption under the *Privacy Act* will no longer apply from 1 July 2026 if the firm provides designated services. All reporting entities will be subject to the *Privacy Act* regardless of size, so newly regulated practices should ensure they understand their obligations in handling client information.

Is there a relevant book, article, film, or podcast you'd recommend to our audience, and why?

For practitioners wanting to understand the human dimension of the law, the stories behind the rules and cases, I return regularly to the *Lives in the Law* podcast by William and Lonsdale. It is a reminder that law is ultimately about people, and that the best lawyers never lose sight of that. The *Lawyers Weekly* podcast series also offers an impressive breadth of perspectives on where the profession is heading. On AML/CTF specifically, AUSTRAC's webinar series is essential. The material is practical, accessible, and directly relevant to the decisions practitioners need to make right now. More broadly, I would encourage lawyers to read (or re-read) the foundational literature on the legal profession's relationship to justice. We are at an inflection point, not just in relation to AML/CTF, but in terms of what the public expects of us. The profession that emerges from this period of change has an opportunity to be defined by its integrity. That is worth reflecting on carefully.

FROM OBLIGATION TO ACTION: MAKING AML COMPLIANCE WORK FOR SMALL BUSINESS

Daniel Mossop | National Manager, Policy Rules and Guidance, AUSTRAC
Alex York | Specialist, Guidance, AUSTRAC

Australia's expansion of anti-money laundering and counter-terrorism financing (AML/CTF) obligations to Tranche 2 industries from 1 July this year is a major legislative reform. In practice, however, it presents a different kind of challenge: a large-scale implementation task, not only for newly regulated businesses, but for the compliance ecosystem that will support them.

International experience shows this transition is rarely straightforward. Across the Financial Action Task Force's fourth round of mutual evaluations, regulators consistently struggled to achieve effective implementation of risk-based obligations in designated non-financial businesses and professions. Levels of risk understanding in key sectors were often low, with only a small proportion achieving 'good' or better ratings across real estate agents, dealers in precious metals and stones, trust and company service providers, lawyers, and accountants. These findings should not be mistaken for lack of intent, but point to broader structural issues. AML/CTF frameworks have largely evolved around the operating environments of large financial institutions – organisations with dedicated compliance teams, in-house legal capability, and the resources to manage complexity. Most tranche 2 businesses operate in very different conditions.

'In Australia, the majority of the more than 100,000 businesses we expect to be captured under the reforms are small businesses.'

Almost all will enter the regime with no prior AML/CTF experience. Many will have limited compliance infrastructure or capacity to interpret complex, principles-based legislation. Without practical support, businesses may default to 'tick-a-box' compliance exercises, adopting inconsistent interpretations or relying on generic, low-quality AML/CTF programs. In these cases, compliance may exist largely on paper rather than in practice, with little impact on reducing risk and community harm. In this context, implementation is not simply about explaining the law more clearly. It is about translating complex obligations into practical steps that can be understood, applied and maintained in day-to-day operations.

It is this combination of scale, complexity and inconsistency that the Program Starter Kits (PSKs) are designed to address, in a world-first initiative for an AML/CTF regulator. These PSKs were released by AUSTRAC on 30 January 2026 and can be found here[1].

[1] https://www.austrac.gov.au/industry-and-business/obligations-and-guidance/program-starter-kits/real-estate-program-starter-kit/real-estate-program-starter-kit-document-library

Developed through AUSTRAC's co-design process with industry bodies, peak associations, expert advisors and businesses, the PSKs respond directly to what small businesses said they needed. The message was consistent: they were not asking for more policy or interpretive guidance, but for practical direction – what to do, when to do it, and how to integrate AML/CTF compliance into the way they already operate.

That challenge is particularly acute in a risk-based regime, where businesses themselves are usually best placed to understand, identify and assess the unique risks they face. Co-design was therefore essential to building a system that could provide clear, scalable pathways to compliance without displacing the need for business-level judgement and tailoring.

'The PSKs provide structured, outcomes-focused compliance frameworks for small, low-risk reporting entities across five sectors: real estate, accounting, legal, conveyancing, and jewellers.'

Available free of charge, each kit includes a risk assessment, a policy document and a process document, supported by a library of forms. Once customised, these components form a complete AML/CTF program.

The tailoring process is central to the model. Businesses must customise the risk assessment to reflect their own services, customers, delivery channels, and risk profile. They must define their risk appetite, determine appropriate controls, and embed those controls into day-to-day workflows. The PSKs are therefore not static templates, but working frameworks that support businesses to build, use and maintain their program over time. In this sense, the PSKs function as an implementation method rather than simply a set of documents. They assume no prior AML/CTF knowledge and build capability through use. By translating hundreds of legislative requirements into structured, accessible formats, they reduce complexity to something manageable. What might otherwise take months can be built and operationalised in days or weeks.

The PSKs reflect a deliberate regulatory approach. In a population of this size and composition, AUSTRAC needed to rethink how it would support implementation at scale across a population inexperienced in AML/CTF. For AUSTRAC, that meant sharing the risk of properly judging and mitigating money laundering and terrorism financing (ML/TF) risks to provide more certainty for business.

'The result is a model that provides clearer pathways for small businesses, leaves room for judgement and risk-based decision-making, and gives AUSTRAC a clear role in continuing to assess risks and update business as ML/TF evolves.'

This shift has implications for consultants and advisers. The PSKs establish a regulator benchmark for practical, small-business implementation. This is likely to challenge parts of the market that have relied on overly generic "off-the-shelf" programs. At the same time, the PSKs clarify where AUSTRAC value sits, making it easier for advisers to build their products from a common base of understanding.

Where AUSTRAC's expectations are clearer, and a practical framework is provided to implement them, less effort is spent interpreting obligations and more can be directed towards helping clients apply them effectively. This includes helping businesses tailor their program appropriately, making sound risk judgements, embedding controls into daily operations, training staff, and responding to emerging risks.

In this way, effort can be directed to where risk actually sits, and to the core purpose of the regime: reducing money laundering, terrorism financing and proliferation financing risks, and the community harm they cause. For more complex entities, advisers will also play a key role in scaling programs beyond the baseline of the PSKs where additional sophistication and controls are required.

Early feedback from across industry suggests the PSKs are being well received and widely implemented, with many providers using them as a foundation to build sector-wide systems to reduce duplication and the costs of compliance.

AUSTRAC will continue refining them over time as businesses begin using them in practice and as implementation issues emerge. This is an important feature of the model: the PSKs are intended to be practical working tools, capable of being refined in response to user experience, emerging and changes in the operating environment. AUSTRAC's co-design process and continuing feedback loops with industry and expert advisor working groups will be fundamental to that approach, supporting a more collaborative and effective response to financial crime risk over time.

Ultimately, the challenge of Tranche 2 is not simply introducing regulation, but ensuring those obligations translate into practical and effective compliance across a large and inexperienced population. The PSKs represent a deliberate attempt to meet that challenge by creating a framework that makes compliance achievable in practice.

Daniel Mossop and Alex York

TRUSTED LEGAL ADVISER AND GATEKEEPER: BALANCING CLIENT EXPERIENCE AND AML/CTF OBLIGATIONS

Carol Prasad | Professional Support Solicitor (AML/CTF), Law Society of NSW

The New Landscape for Lawyers

The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) extends obligations (known as Tranche 2 Reforms) to gatekeeper professions, such as lawyers, who provide one or more *designated services* from 1 July 2026. A *designated service* is defined in section 6 of the AML/CTF Act, and for lawyers, this could include conveyancing, transactional work, including equity and debt financing, or certain commercial transactions. For Australian lawyers, these reforms introduce some of the biggest changes to practice in decades. Lawyers often sit at pivotal points in transactions including property, corporate structuring and trust arrangements, all of which have been recognised as being vulnerable to criminal misuse. Understandably, there is some concern across the profession about how Tranche 2 Reforms will affect the traditional lawyer-client relationship.

'The focus for many is not just on compliance with the new regime, but how to assure clients of the ongoing fiduciary relationship, as well as advance broader societal outcomes through the reduction of financial and criminal harms.'

Customer Due Diligence and The Client Experience

A key obligation under the AML/CTF legislation is customer due diligence (CDD). This is not a new concept for lawyers. The legal profession has long operated on the principle of knowing the client. Lawyers are expected to understand who they act for and identify conflicts. What will change is the level of effort required, as CDD is based on risk factors, including customer risk, channel risk, geographic risk and matter or transaction risk. The reforms also introduce record keeping requirements and regulatory expectations around those processes. There are consequences where processes fall short of those expectations.

The impact of these structured requirements on the day-to-day operations of legal practices is real. The obligations are complex, and it may increase costs and time spent on onboarding clients. There could be delays, impacts to existing client relationships and, in practical terms, some costs may need to be passed on to clients. Practices will also need processes for the ongoing monitoring of clients, training of staff, and considering obligations under the *Privacy Act 1988* when collecting personal information from clients and related parties. The use of technology can streamline CDD processes, but this too may come with additional costs. Where the technology is provided by a third party, practices will need to CDD on that provider and thoroughly review service agreements. More broadly, captured industries will need to turn their mind to opportunities to avoid duplication of processes, particularly in typical conveyancing and real estate matters where multiple service providers, for example lawyers and real estate agents, involved in the same matter, may separately interact with, and need to verify the same client. Where relevant, this can be facilitated by having in place reliance agreements.

Why Framing Matters

Clients are no strangers to providing CDD information, including to financial institutions. With Tranche 2 Reforms, clients will need to provide certain information to an extended group of professionals, including, for example, their accountant, real estate agent, conveyancer and/or lawyer. At their heart, CDD measures are designed to verify the client's identity, and to identify and assess the money laundering (ML), terrorism financing (TF) and proliferation finance (PF) risks when providing designated services. These requirements are not merely bureaucratic. They are aimed to detect impersonations, potentially identify scams and fraud, and disrupt ML/TF/PF and related crimes.

For the legal profession, how AML/CTF obligations are explained to clients will matter enormously. Clear messaging will form the basis of the evolving professional and regulatory landscape and significantly reduce resistance. In addition, clear internal systems and processes will ensure that work can flow with minimum disruption. Importantly, balancing the client experience with AML/CTF obligations does not mean abandoning empathy or trust.

'Lawyers routinely navigate difficult conversations, whether this is about litigation risk, commercial realities, or legal fees. Communication about CDD, and more generally about the firms AML/CTF obligations, can be handled in the same professional way.'

Culture at The Heart

Ongoing investment in people will be at the heart of establishing a strong AML/CTF culture within the firm. AML/CTF training is a legal requirement, but on its own is unlikely to be as effective as the firm's overall culture. This includes a 'tone-from-the top' that does not focus merely on rigid compliance and penalty avoidance, but also on reduction of societal harm. AUSTRAC has highlighted the importance of governance, leadership, and culture in driving meaningful compliance, and said that a "strong AML/CTF culture isn't a legal requirement but is often a reliable driver and indicator that your business is taking reasonable steps to meet its obligations. We'll look for evidence of such a culture in our supervision."

Embedding AML/CTF into Modern Legal Practice

Change of the magnitude created by Tranche 2 Reforms will be disruptive. The reforms create practical challenges for practices, including for sole practitioners and smaller firms, that must now, for the first time, navigate not just the AML/CTF regime but also privacy obligations, while maintaining their day-to-day practice. But they also reinforce principles that lawyers value, including integrity and maintaining confidence in the legal system. There is also a broader societal impetus that matters. Effective AML/CTF frameworks across the captured legal population and other gatekeepers will go a long way in deterring, detecting, and disrupting serious and organised crime.

The NSW Law Society has developed its AML/CTF Hub[1], a comprehensive online resource, that is continually updated and designed to help legal practitioners prepare for and comply with Tranche 2 Reforms. Ultimately, firms that adapt to the changes most effectively are likely to be those that integrate AML/CTF into their broader professional, governance and risk management frameworks. In doing so, the profession has an opportunity to demonstrate its ongoing role in safeguarding the integrity of financial and legal systems.

[1] https://www.lawsociety.com.au/practising-law-nsw/aml-ctf-hub

TIPPING THE WINK: WHAT DISCLOSURES OFFEND S 123 AML/CTF ACT?

Dr Mathew Leighton-Daly | Special Counsel, HWLE Lawyers; Visiting Academic, University of Sydney Law School; Industry Fellow, Academy of Excellence in Financial Crime, Griffith University

Although the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act) primarily imposes civil obligations in relation to anti-financial crime, it contains some criminal prohibitions. The Offence of 'tipping off' under s 123 of the AML/CTF Act is one such prohibition. Tipping off refers to the illegal act of disclosure by an entity to a customer or third party that a suspicious matter report (SMR) has been filed or certain other disclosures have been made. The offence is punishable by way of imprisonment for 2 years and/or 120 penalty units. The offence applies to all reporting entities (and certain associates), which obviously includes tranche 2 entities. This work explores the scope of the prohibition by reference to two key steps or enquiries: disclosure and prejudice.

Prior to 31 March 2025, the prohibition on tipping off was drafted in very broad terms. Here a reporting entity could not disclose to a person (other than AUSTRAC), any information from which the person to whom the information is disclosed could reasonably be expected to infer that information had been communicated to the AUSTRAC as a SMR, or that a suspicion has been formed. The reasonable inference element was sometimes, colloquially, referred to the inferential test.

'Not surprisingly, the inferential test resulted in over criminalisation and prohibited disclosure in a plethora of benign situations.'

With effect from 31 March 2025, the 'tipping off' offence was substantially amended. Notably, the inferential element was repealed the offence recast to focus on whether a disclosure 'would or could reasonably prejudice an investigation'. The current offence does not only apply to reporting entities themselves. It also applies to a person who is or has been one of the following:

- an officer, employee or agent of a reporting entity;
- a member of a reporting group;
- an officer, employeeor agent of a memberof a reporting group;
- required by a notice under subsection 49(1) togive information or produce documents; or
- required by a notice undersubsection 49B(2) to give information or produce documents.

The logic behind the inclusion of 'is or has been'in subsection 123(1)(a) is to ensure that even when a person ceases to be a person described in the list that the prohibition on disclosure of information is enduring.

The first key step or enquiry in relation to s123 is in relation to disclosures by the persons covered above. Subject to the prejudice test (discussed as step 2 below) the following disclosures are prescribed as being prohibited:

- where a reporting entity has given,or is required to give,a SMR;
- a SMR itself;
- a copy of the SMR;
- a document purporting to set out information (including the formation or existence of a suspicion) contained in an SMR;
- disclosures under Division 6;
- information referred to in paragraphs 16(5A)(a), (b) or (c) or (5AA)(a) or (b) of the FTR Act, as in force immediately before its repeal.

The words in the current s 123(2)(d), namely, "(d) a document purporting to set out information (including the formation or existence of a suspicion) contained in such a report;" are identical to the words used in s 16(5D)(iii) of the now-repealed Financial Transaction Reports Act 1988 (FTRA). The FTRA provision was the subject of consideration by the Full Federal Court in Colonial Mutual Life Assurance Society Ltd v Donnelly [1998] FCA 364. In this case, the primary Judge admitted into evidence, without objection, annexures to the affidavit of an AUSTRAC officer, including a report on a "suspect transaction" made by her under the FTRA.

The Court held:

> *In our view, [the FTRA PROVISION] is intended to exclude a document purporting to recount what has been said in a report under the FTR Act. That is, it is intended to supplement sub-pars (1) and (ii) of s 16(5D)(a), which exclude the report and any copy of the report, by making inadmissible secondary evidence of the contents of any report. The legislation is not intended to preclude a person giving direct evidence of what he or she saw or did, simply because some of that evidence happens to recount the same events referred to in a report under the FTR Act. Thus, the direct evidence given by Ms Johnson was not rendered inadmissible … the FTR Act.*

The scope of potential prohibited disclosures beyond the SMR and its contents then appears to be limited to the purported contents of an SMR or, in other words, information from which the person may make the connection between the information they have been given and the fact/contents of an SMR.

The second key step or enquiry under the current s 123 is the element/test of prejudice. Butterworths Australian Legal Dictionary defines prejudice to relevantly mean "[t]o harm or injure another's rights." The inclusion of 'would or could reasonably be expected to prejudice' in paragraph 123(1)(d) captures both intentional and reckless disclosures.

In relation to intentional disclosures, the Explanatory Memorandum (EM) notes that disclosure would or could reasonably be expected to prejudice an investigation where a reporting entity notifying a customer who is the subject of a SMR or their known associate that a suspicion was formed in relation to their behaviour and a SMR has been submitted. This kind of disclosure risks criminals taking action to hide or disguise their illegal activities. As for reckless disclosures, the EM explains:

> *For example, the offence would cover a disclosure as a result of a lead entity or other reportingentity's failure to develop, implement or maintain appropriate AML/CTF policies to prevent tipping off when sharing within a reporting group.'*

Section 123 contains its own express exceptions to the offence. Apart from those disclosures too falling outside the scope of subsection 123(2) AML/CTF Act, guidance has been provided in relation to the prohibition won't apply.AUSTRAC's view is consistent with the EM but is expressed in more detail. These include:

- to comply with requirements in Commonwealth, State or Territory laws. For example, laws to prevent scams, such as the Scams Prevention Framework, or state-based gambling laws
- to appropriately manage ML/TF risks in your business. For example, disclosures to staff or senior management in your business, a reporting entity in your designated business group or corporate group or external service providers for this purpose
- in the process of supporting due diligence in a merger or acquisition involving your business
- to meet your AML/CTF obligations or manage ML/TF risks. For example, to consultants supporting you with AML/CTF remediation and uplift, or to your lawyer to seek legal advice on your AML/CTF obligations
- to participate in activities of the Fintel Alliance, including through disclosures made between reporting entities engaging in these activities
- if your SMR obligation has not been triggered and you are asking a customer reasonable questions or conducting enhanced customer due diligence.

Importantly, the fact of an investigation is not the relevant test here. Subsection 123(3) provides that it is immaterial whether an investigation has commenced. According to the EM, this is intended to clarify that a reporting entity does not need to know that an investigation is underway. In non-obvious cases (e.g. disclosure to law enforcement and regulatory agencies) this element/test will likely have to be considered on a case-by-case- basis.

The two-step approach set out above seeks to clarity the scope of the tipping off provision.The breadth of the enquiry in step 1 as it relates to applicable persons is mitigated by the prescriptive approach to articulating the specific instances of disclosures that are prohibited.Since the repeal of the inferential test and having regard to the common law on an identical provision to that in the current subsection 123(2), this is quite narrow. The second step's test of prejudice narrows the provision further however the requirement for objectivity - except in obvious case - may lead to uncertainty.

Mathew Leighton-Daly

MOVING PROFESSIONS FROM GRIEF TO ACCEPTANCE IN THE AML/CTF JOURNEY

Alice Saveneh-Murray | Financial Crime Partner at KordaMentha

Lawyers, accountants and real estate agents are just some of the professionals soon to be brought into scope under the second tranche of Australia's anti-money laundering/counter-terrorism financing (AML/CTF) laws.

'For many, the immediate reaction will be a mix of frustration and fatigue. But the more useful question is why these professions sit so squarely in the policy intent. By doing this, Reporting Entities can move past their initial reactions and focus on what this looks like in practice.'

Why Professionals Are Now In Scope

Lawyers, accountants and real estate professionals are referred to as gatekeepers in the money laundering chain, because they are often involved well before a transaction takes place. This means they have a chance very early on in a transaction to observe indicators that suggest heightened money-laundering/terrorist-financing (ML/TF) risk. Given their role in establishing and managing client structures, gatekeepers may also at times have direct contact with individuals or representatives of who seek to use those structures for illicit purposes, including receiving instructions from them.

While banks see the funds move, gatekeepers are the ones that see how the structures are set up and the intent behind them. That is the gap regulators are trying to close. There is clear evidence this gap has been exploited in Australia, with the Australian Transaction Reports and Analysis Centre (AUSTRAC) and law enforcement identifying repeated use of professional facilitators and corporate structures to disguise and move illicit funds.

The regulator, AUSTRAC, expects reporting entities' business processes to account for and mitigate the potential for criminals to launder money through their operations. A practical starting point for new reporting entities is to understand how the behaviours and activities that have driven these reforms arise in practice, and ensure their own services cannot be used in the same way.

From Obligation to Practical Response

The risk assessment sits at the core of an effective response to the new AML/CTF requirements. It cannot be treated as a theoretical or tick the box exercise. To be meaningful, the assessment must articulate that the business understands its role within potential criminal activity and where its services could be misused.

This requires more than just describing products or client types. It must reflect the risk embedded in how services are actually delivered, how your clients operate and how transactions unfold in practice. It should also recognise where those models could be vulnerable to exploitation, the moments in a transaction cycle that can be manipulated and the signals that tend to precede them.

Importantly, AUSTRAC's expectation is not uniformity but proportionality. Firms are not expected to replicate the scale or complexity of a major bank's compliance function, but they are expected to understand their exposure and respond accordingly.

In this new environment, hand holding from the regulator on day one is impractical. With tens of thousands of new entities now under its remit and limited time to oversee them, AUSTRAC will be relying on firms to make reasonable, defensible decisions from the outset. It's also unlikely they will be immediately applying a harsh lens to entities that are trying to do the right thing. That is why a simple, repeatable AML/CTF program is ideal and will make it as straightforward as possible to demonstrate compliance if and when the regulator has a query.

Our experience and observations suggest you will have the greatest success when you build new controls into existing workflows, rather than trying to create whole new processes or deploy an 'out of the box' solution. Most businesses will already have established processes for onboarding clients and monitoring their relationships. The expectation now is that you have a way to flag concerns that may arise if red flags in those processes present themselves.

'Be cautious of solutions that promise rapid or simplified compliance outcomes without a clear link to how their business actually operates. In practice, frameworks that are not grounded in your specific risk profile are difficult to sustain and even harder to defend under scrutiny.'

The test you should apply is whether decisions you make now can be explained in a consistent and defensible way 5 or 6 years from now. If the system is overcomplicated, you are inviting multiple points of potential failure and if your initial decisions and rationale go undocumented, you may find it very difficult to defend future issues or scrutiny.

Where Firms Are Getting Stuck, and What To Do About It

Despite seeing uneven degrees of acceptance and readiness across the soon-to-be regulated population, there are already some common challenges emerging. Many firms are aware of their obligations in principle but are struggling to translate them into day-to-day processes. This 'knowing versus doing' gap is where many firms are getting stuck, and implementation to practical forms and decision-making frameworks stalls.

Conversely, some firms are responding by over-engineering their frameworks. Extensive documentation and layered processes can create complexity without improving outcomes. In practice, this can introduce more points of failure and reduce consistency in execution. Simpler, well understood processes that align to how the business actually operates tend to be more effective and more defensible. This is especially important when you consider the responsibility for execution is likely to be sitting with people who are new to compliance. We cannot underestimate the demand these reforms will create for experienced AML/CTF staff and the challenge that will present for all reporting entities when it comes to talent attraction and retention.

One final suggestion for firms about to embark on AML/CTF compliance: don't forget to tell your clients about what is coming. To date, despite a lot of valuable guidance to reporting entities, there has been very little public awareness on the reforms and how they will impact individuals wanting to access services in the accounting, real estate and legal sectors. This will be a tricky aspect to manage, given how much emphasis is rightly placed on protecting the general public from fraud, scams and cyber security.

Consumers have become used to KYC procedures associated with financial services, but they may be naturally reticent to hand over information of a personal nature unless you are clear about the obligations you are now subject to and can provide them with adequate comfort on your security protocols and how you will protect their confidential information. This is especially true if you are asking them to provide identification details online and/or through third parties – yet another barrier for professionals to overcome on their road to compliance.

The Road to Acceptance

These reforms will test how firms respond to change Initial frustration with these reforms is to be expected, but remaining there misses the point of why these professions have been brought into scope. Acceptance comes from taking ownership of the risk and embedding controls that work in practice. The sooner that shift happens, the more straightforward compliance becomes.

Alice Saveneh-Murray

CONSTRUCTING COMPLIANCE AS LEGAL CULTURE: ASSESSING THE POTENTIAL FOR MORE EFFECTIVENESS

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

Introduction

The reporting obligation for professions in the context of the implementation of the anti-money laundering (AML) regime still leaves questions and complaints related to the secrecy of certain professionals as mandated as a reporting party; the shift of the burden that originally belonged to the state was transferred to the professions, and may also be related to the difficult task of revealing beneficial ownerships. In particular, in the context of Indonesia, the laying of this obligation is not regulated in a law, but is only mandated in Article 17 paragraph (2) of the law related to money laundering, and which is then regulated in a government regulation. It is a crucial problem where the special rules related to the profession regulating the secrecy of the profession are regulated in the form of a law, whose position is above government regulations. In addition, the imperfect understanding and implementation of Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) will be a difficulty in itself.

In the very rapid economic development, money laundering poses a very serious threat to the country's financial stability and global security. This development puts the AML regime at the forefront of being strengthened by the international community and the country. One aspect of the AML regime is the obligation to report for professionals, who are recognised as the reporting party, who, in this case, are always directly confronted with the issue of the profession's secrets. In this case, even if there is protection for the reporting party from civil lawsuits or criminal charges for the exception of the disclosure of office secrets, when the reporting party does so in the context of implementing the order of the money laundering law, it is not an act of abuse.

Specific Professions, Reporting Obligations, and the Meaning of Professions' Secrecy

Professionals' secrecy contains a moral and legal obligation. A certain profession under the AML regime, such as lawyers, notaries, accountants, appraisals, is obliged to maintain the confidentiality of the information they obtain from clients. The obligation is aimed at the value of trust, which must always be built between the client and the profession. It is also used to ensure that clients provide the necessary information without any suspicion or worry that the secret will be leaked or known to other parties.

In the anti-money laundering and counter-terrorist financing (AML/CTF) framework, the secrets of the profession become, and always will be, a complex problem; these professions have their objections. However, in its development, these professions have played a significant role as gatekeepers. In the context of the AML regime, various types of financial transactions are known, namely suspicious financial transactions, cash financial transactions, and fund transfer financial transactions.

On the other hand, the reporting obligation, which has the dimension of criminal and administrative sanctions, is felt to be contrary to the confidentiality of the position, in which case the obligation requires the professional to disclose information that may be confidential, which is limited to certain points, but still requires analysis in carrying it out.

The other main pillars in the AML regime are the reporting obligation of reporting parties. They are required to identify, verify, and monitor transactions to their supervisory and regulatory institutions.

'This obligation requires vigilance in identifying suspicious activity and conducting appropriate risk assessments. In some respects, this creates tension between ethical and legal obligations, particularly in relation to a professional's secrecy.'

These professions must strike a balance between maintaining client confidentiality and fulfilling their legal obligations. In this case, conflicts arise, which bring uncertainty to the profession. Therefore, in overcoming this, a special exception is set to report without worrying about violating confidentiality obligations. The law protects by releasing the possibility of civil or criminal prosecution for the professional.

CDD and EDD Implementation: Is it Difficult?
CDD and EDD are significant aspects of money laundering prevention efforts. CDD and EDD are used to ensure that transaction activities are carried out in accordance with the risk profile they have. CDD and EDD are important for the reporting party, in this case, a professional, who is specifically intended to maintain financial integrity. These professions are often considered gatekeepers because of their expertise and access to financial transactions, and the establishment of business entities, which have the potential to be used by criminals to disguise the proceeds of crime. Both are efforts to mitigate risks as well as protect the reputation of the profession, so it requires understanding the objectives of business relationships, as well as assessing the risk profile of the client.

However, implementing CDD and/or EDD also requires a strong will. One of the difficulties in implementing CDD and/or EDD is determining the level of customer risk accurately. Collecting valid data and maintaining the integrity of information is also a challenge in itself. These professionals must always update their knowledge as regulations and technology change.

Initiating Self-Risk Assessment and Reporting Compliance as a Legal Culture
A strong compliance culture and independent risk assessment will be an important element in combatting money laundering in the reporting dimension. Professionals must have a deep understanding of the risks of money laundering that may be encountered in their work, as well as implement appropriate preventive measures.

To build compliance as a culture, it needs to involve adequate training in certain professions, and the ability to diagnose which transactions are risky for them. Professionals are encouraged to report suspicious activity of their clients without fear of retaliation.

An effective risk assessment allows professionals to focus on areas of high risk and take appropriate precautions. In this case, professionals will not solely do so by just doing their obligations, so they only focus on the formalistic fulfilment of obligations, not the substance of why it is important to carry out prevention. It will also help fulfil the obligation to report as an awareness to report, not just because it is required. It is also not solely seen as a potential legal sanction as a threat, but as a support for the protection of the state. Professionals do not hide behind the fear of breaching professional secrecy.

‘The Financial Action Task Force, together with countries, needs to consider clarifying legal exceptions that permit reporting without breaching professional secrecy obligations, thereby providing greater legal certainty for professionals. .’

By building a strong legal culture of compliance, as well as the ability to conduct appropriate self-risk assessments, and the adoption of a balanced approach, professionals can contribute significantly within the framework of the AML/CFT regime, rather than just shifting the burden from the state to professionals. By fostering the self-risk assessment framework as a legal culture rather than obligations that may still have an impact on the imposition of sanctions, these professions are expected to be able to assess exactly what they should do, so that they are not exposed to the risk of money laundering in the effort to carry out their work within the framework of the anti-money laundering regime. Thus, it is hoped that it can be more effective.

Go Lisanawati

REGULATING THE GATEKEEPERS: FOLLOWING THE MONEY BEHIND ORGANISED CRIME

Katie Bourne | Director, Forensic Services, BDO
Huey Lam | Senior Manager, Forensic Services, BDO

'In nearly two decades working in organised crime investigations and asset recovery, one theme has remained constant: organised crime's greatest vulnerability is its money. Criminal enterprises exist to generate profit, and as long as that profit can be concealed and enjoyed, the underlying incentives remain intact.'

In Australia, professional 'gatekeepers', including lawyers, accountants, real estate agents, and other advisers, have helped criminals hide and move illicit wealth with impunity. Operating beyond the scope of anti-money laundering and counter-terrorism financing (AML/CTF) obligations, these professionals have leveraged a regulatory gap, allowing criminals to obscure beneficial ownership, move funds through legitimate structures, and integrate illicit wealth into the financial system. This is not a minor loophole; it is a chasm in our defences.

From an investigative perspective, this gap not only complicated prosecutions but also shifted the balance of power between criminals and the state. When professional expertise is used to shield illicit wealth, even the most sophisticated investigative efforts can be delayed, diluted, or ultimately undermined.

Critically, the professional enablers are rarely naive or ignorant. They are often brazen opportunists who know exactly what they are doing. Commanding high fees, some knowingly collude with criminals or turn a deliberate blind eye, sacrificing ethics for profit. A lack of regulatory clarity has reinforced the perception that risk sits with their clients, not with themselves. Until recently, many have assumed, often correctly, that enforcement attention would focus on principal offenders rather than the those enabling them. In the absence of AML/CTF obligations, this dynamic has fostered a shadow service economy that supports and sustains the growth of illicit enterprises.

The Hidden Power of Professional Facilitation

The role of professional enablers in shielding and enabling illicit wealth is not abstract, it plays out in real investigations. This dynamic was clearly demonstrated in a case we both worked on, where a long-running money laundering and tax evasion investigation revealed just how effectively a single facilitator can enable and sustain complex criminal activity over time. The principal architect built a clandestine business that enabled dozens of clients to evade taxes and launder undeclared income, in exchange for a commission on the funds processed.

The scheme operated over many years and depended on a professional facilitator: an accountant who established shell companies with no legitimate commercial purpose, used to obscure beneficial ownership, conceal the source of funds, create a veneer of legitimacy for financial flows, and coordinate efforts to stay ahead of regulatory and law enforcement scrutiny.

These tactics allowed wealth to be moved and concealed at a pace that outstripped conventional tax enforcement processes, creating a sustained cat-and-mouse dynamic that proved difficult to disrupt using traditional tools alone. It ultimately took a full-scale joint law enforcement operation, including forensic asset tracing, to untangle the web and restrain proceeds. By that time, however, much of the profit generated had already been dissipated or reinvested into assets including, gold bullion or property.

This case reinforced a sobering reality: the longer criminals can obscure their financial footprints, the harder it becomes for authorities to restrain and recover illicit profits. From a policy perspective, this is significant. Targeting individual criminal enterprises may disrupt specific operations, but addressing the facilitation layer has the potential to generate broader systemic impact.

Does Regulating Gatekeepers Meaningfully Reduce Global AML/CTF Risk?

Regulating professional services will not eliminate criminal misuse, but it introduces friction that makes reliance on professional facilitation significantly harder to sustain.

The case described illustrates why that distinction matters. The accountant at the centre of the scheme operated in an environment where there was no obligation to interrogate who the real client was, why complex structures were required, or whether the movement of funds aligned with any legitimate economic purpose. Their business model depended on speed, opacity, and the absence of scrutiny.

Had customer due diligence and ongoing risk assessment obligations applied at the time, that model would have been far more difficult to maintain. Phoney trusts and companies, along with complex transactions lacking any economic rationale would have required explanation. Implausible source-of-funds narratives would have needed to be documented or rejected. At the very least, the accountant would have been forced to reassess whether the commercial upside justified the regulatory and reputational exposure.

Shifting the Operating Environment

The AML/CTF Tranche 2 implementation changes mark a structural shift to the dynamic. Criminals can no longer assume their lawyer, accountant, or fixer can quietly manage illicit activity behind closed doors. Regulators and law enforcement, armed with greater visibility into these sectors, will have stronger grounds and better data to act when facilitators cross the line.

Even modest levels of scrutiny can disrupt criminal methodologies that rely on speed, secrecy, and professional complicity. Transactions that would previously proceed without question may now be delayed, interrogated, or abandoned altogether. Structures designed to obscure ownership may become more difficult to establish and maintain.

In response, firms begin to reassess the clients and engagements they are prepared to accept. Risk appetite narrows, high-risk work becomes commercially unattractive, not because it is expressly prohibited, but because it carries scrutiny, documentation and accountability that many facilitation models cannot withstand. As a result, criminal clients encounter fewer willing intermediaries, higher costs, slower execution, and a significantly increased likelihood of exposure.

AUSTRAC's Money Laundering Update 2026 reinforces why this shift is important. It highlights that core money-laundering channels are becoming more complex and interconnected, with professional facilitation remaining an enduring vulnerability rather than a legacy risk, one that is further amplified by technology. The introduction of AML/CTF obligations removes critical blind spots that have historically allowed facilitators to operate undetected.

Closing the Gaps

These reforms do not close every door, but it will close enough to materially alter the operating environment. From both investigative and asset confiscation perspectives, that shift is meaningful. It weakens the scaffolding that allows criminal wealth to be normalised within the legitimate economy, forces illicit activity into less efficient and more detectable channels, and increases the likelihood that proceeds can be identified, restrained and ultimately removed.

'Delays and extra scrutiny can disrupt a criminal operation's cash flow, buying investigators valuable time to detect patterns and trace assets before they are dissipated.'

Regulating the gatekeepers is not a silver bullet. However, by following the money into the professional environments where it has historically been safest, and by forcing facilitators to confront their own risk exposure, it targets the systems that allow financial crime to persist. In that sense, it represents one of the most consequential structural reforms in the global AML/CTF landscape.

Katie Bourne and Huey Lam

WHEN COMPLIANCE LOOKS RIGHT BUT FAILS: THE REAL RISK BEHIND TRANCHE 2 REFORM

John Kouroutzoglou | Cybersecurity and Financial Crime Specialist, Founder, Secure Tactix

There is an uncomfortable truth sitting beneath Australia's Tranche 2 reforms. Financial crime does not succeed because rules are missing. It succeeds because, at critical moments, those rules are not applied. Those moments do not occur in policy documents or training sessions. They occur in conversations, transactions and decisions made under pressure. And pressure is exactly what many of these sectors are operating under.

For decades, Australia has operated with a significant blind spot in its anti-money laundering (AML) framework. While financial institutions have been heavily regulated, entire sectors responsible for structuring transactions, moving assets and enabling ownership have remained outside the regime. Real estate agents, lawyers, accountants and dealers in precious metals and stones have historically not been required to conduct meaningful due diligence or report suspicious transactions.

This gap has not gone unnoticed. Australia has, at times, been grouped alongside jurisdictions such as Cambodia and Haiti in failing to regulate these gatekeeper professions under anti-money laundering and counter-terrorist financing (AML/CTF) frameworks. That comparison is uncomfortable. But it reflects a simple reality.

For years, Australia has been an attractive destination for illicit funds, not because of weak institutions, but because of gaps in how those institutions connected. Tranche 2 is an attempt to close that gap. But regulation introduced late is often introduced into environments that were never designed for it. Those environments are already under strain.

Real estate agents are operating in a tightening or volatile market. Dealers in precious metals and stones face intense competition in cash-heavy environments. Professional service firms are balancing client expectations with rising compliance obligations. Add cost-of-living pressure and something subtle begins to shift. Standards do not collapse overnight. They erode.

'A client becomes a '"good opportunity".
A question becomes "not worth asking".
And eventually, money becomes just money.'

Australia already knows where the vulnerabilities sit. Real estate has long been identified as a preferred channel for laundering illicit funds, with billions in criminal proceeds flowing through the sector. Property offers scale, stability and legitimacy, allowing illicit funds to be absorbed into the economy in a way that appears clean.

More broadly, traditional methods continue to dominate: cash, property, luxury goods and professional services. Not because criminals lack sophistication. But because these channels work. The real vulnerability is not just structural. It is behavioural.

Consider the moment a transaction is about to close. The deal has taken weeks, sometimes months. The client relationship is established. Revenue is within reach. And something does not quite add up.

'At that point, the decision is rarely framed as 'comply or break the law.' It is framed as something far more human: Do I push this further and risk losing the deal, or do I accept what I have been given and move on?'

Financial crime rarely forces its way into a system. It is allowed through, one reasonable decision at a time. This is not theoretical. Recent Australian Federal Police investigations show how financial crime operates at scale, and often in plain sight. Authorities have restrained more than $1.1 billion in criminal assets over a four-year period, with syndicates laundering hundreds of millions through business networks operating across the country. In some cases, more than $10 billion moved through exchange networks, operating openly through legitimate-looking shopfronts.

The proceeds follow a familiar pattern. Illicit funds are converted into residential property, luxury vehicles, high-end goods, financial assets. Assets that provide both value and legitimacy. This reflects a system where funds can move through multiple layers of professional and commercial activity without consistent challenge. Financial crime does not need to hide. It only needs to be accepted.

This is where a critical assumption emerges. There is often an expectation that financial institutions will act as the primary line of defence. Banks are expected to detect unusual patterns, challenge source of funds and escalate suspicious activity. From a commercial perspective, this assumption is convenient. But it is flawed.

By the time funds reach a bank, key decisions have already been made. The client has been accepted. The structure has been established. The transaction has been legitimised. Risk has not been managed. It has been passed on.

There is also a broader structural tension. Property transactions are a major source of government revenue, particularly through stamp duty and related taxes. This creates a balancing act. On one hand, regulators seek to strengthen controls and disrupt high-risk transactions. On the other, those same transactions contribute to economic activity and public revenue. This does not imply misplaced priorities. But it does highlight a system where strong incentives exist to keep transactions moving. Where that is the case, controls must work harder to interrupt them.

Some sectors face this challenge more directly. In real estate, high transaction values and limited visibility over source of funds create natural exposure. There is also a tendency to assume that responsibility sits elsewhere in the chain.

In precious metals and stones, the exposure is even more direct. These assets are portable, high-value and easily transformed, making them attractive for storing and transferring value with limited traceability.

In both cases, the system does not need to fail completely. It only needs to allow one transaction to pass without sufficient scrutiny.

This is how gatekeepers fail. Not through deliberate wrongdoing. But through small decisions:

- not asking the second question
- accepting incomplete explanations
- assuming someone else will carry the risk

Individually, these decisions appear reasonable. Collectively, they create pathways. None of this suggests that professionals are complicit. But it does highlight something more difficult to confront.

'Financial crime does not require intent. It requires tolerance. Hesitation. Assumption. Convenience.'

As economic pressure increases, so does the likelihood of these behaviours emerging. Tranche 2 reform is designed to address these risks. The intent is sound. But intent alone does not close gaps. Its effectiveness will depend on how individuals respond in those moments where commercial pressure and compliance obligation collide.

If compliance remains procedural, it will fail under pressure. If it becomes part of professional judgement, it has a chance. Money laundering is not an isolated offence. It enables broader criminal activity and sustains organised crime. If the money moves, the system works for those exploiting it.

Tranche 2 is not just a compliance exercise. It is a test. Because when the pressure is on and the deal is in front of you, the real question is simple: 'Do you ask the hard question, or do you let it pass.

John Kouroutzoglou

MAKING THE NEW EU AML AUTHORITY COUNT: THREE TESTS

Sunny Nagpal | Senior Solutions Lead, Symphony AI

There is a visible and growing movement globally to bring professional service providers -accountants, lawyers, conveyancers, real estate agents; under anti-money laundering and counter-terrorism financing (AML/CTF) regulation. The logic is straightforward: these professions sit at the frontline of financial transactions, and for too long they have operated outside the regulatory perimeter that financial institutions have been held to for decades. FATF has been pushing this for years. Australia has now legislated it. The UK is consolidating supervision under the Financial Conduct Authority (FCA). The EU is standing up an entirely new authority. The direction of travel is clear.

'So why am I not yet convinced this will deliver on its promise?'

Not because the policy direction is wrong. It isn't. These professions do get used to move dirty money, through law firm trust accounts, through property settlements, through structures that look legitimate on the surface. The case for regulation is clear. My concern is narrower: we are spending enormous energy debating who gets regulated, while largely underweighting the harder question of how that regulation will actually be operationalised and supervised at scale.

After nearly two decades delivering and supporting AML/CTF transformation programs across Tier-1, Tier-2 banks and financial institutions, and watching the compliance infrastructure those programs required up close, I want to share a practitioner's concern that doesn't get much airtime: the harder problem isn't the legislation. It's what happens the day after it takes effect.

The Gap Between Obligation and Reality

Consider what Australia has done. The Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2024 is a genuine reform; carefully designed, long overdue, and broadly aligned with FATF expectations. From July 1, 2026, accountants, lawyers, real estate agents, and others will carry formal AML/CTF obligations for the first time. Risk assessments. Customer due diligence. Suspicious Matter Reporting. An entire compliance architecture that the financial sector has spent decades and hundreds of millions of dollars building, now expected from a sole-practitioner conveyancer in Wagga Wagga.

I do not say this to be dismissive of those practitioners. Many I have spoken to are approaching their obligations with genuine seriousness. But seen inside these programs firsthand where they struggle; in-fact organisations with dedicated compliance teams, enterprise tech stacks, and significant experience behind them, find it difficult to operationalise a risk-based compliance program that works. The gap between a policy document and a functioning control environment is vast. That gap is where financial crime hides.

To make that concrete: I once worked on a control's harmonisation program at a major Australian financial institution, an organisation with a full compliance function, dedicated risk teams, enterprise technology, and years of regulatory engagement behind it. One of the most consuming exercises in the entire program was simply agreeing on what a control was. What it covered. Who owned it. Whether it was operating as intended. Whether the risk it was supposed to address was genuinely being managed. Not designing new controls. Not implementing new platforms. Just achieving shared, honest understanding of what already existed.

That process involved months of cross-functional workshops, genuine disagreements between business lines and second-line risk, and significant senior leadership time before anyone felt confident in the picture. It was valuable – it surfaced gaps that nobody had clearly owned – but it was also deeply hard, in an organisation with every structural advantage you could ask for.

Now apply that same exercise to a four-person accounting practice. No compliance function. No risk team. No prior experience of this regulatory environment. The obligation is real, the framework is published, and the intent is genuine. But the operational reality of knowing what your controls are, who owns them, and whether they're working? That requires capacity these entities simply don't have and no guidance document, however well-written, fully bridges that gap.

AUSTRAC is an excellent regulator. But it is difficult to see how any regulator could meaningfully engage with 100,000 new reporting entities, most of them small businesses encountering AML/CTF obligations for the first time, in a compressed timeframe.

A Question Worth Considering

Two approaches offer an instructive contrast. The UK has moved to consolidate AML supervision of legal, accountancy, and trust and company service providers under a single supervisor 'the FCAA' arguing that fragmentation across multiple professional body supervisors produced inconsistent standards. Australia has kept AUSTRAC as primary supervisor across all newly regulated entities, an agency with genuine credibility from decades of enforcement that has transforming compliance culture inside major institutions.

Both are defensible. But I keep coming back to something I have observed consistently inside institutions: compliance culture tends to reflect the intensity of supervisory pressure around it. Where that pressure is high and sustained, the culture shifts. Where it isn't, the early habits, however well-intentioned, tend to stick. How those dynamic plays out across 100,000 small businesses, most of them encountering these obligations for the first time, is a question I don't think has a clean answer yet.

What the Implementation Actually Could Be

This is probably obvious to anyone who has worked in compliance for long enough: when new obligations land, there is an initial surge of activity. Policies get written, training gets delivered, systems get procured. But what's harder to build and what tends to be missing years later is the judgment and the daily habit of applying these principles to real client decisions. The paperwork gets done. The culture takes much longer.

At major Australian financial institutions, that culture shift took years of sustained engagement and, in several cases, significant enforcement attention before it became genuinely embedded. Professional service providers will not have that same supervisory pressure, at least not initially. Which means the compliance culture that forms in the first two to three years will be shaped primarily by peer norms and whatever guidance professional associations, CPA Australia, the Law Council, the Real Estate Institute, choose to actively push.

Whether those bodies step into that role meaningfully, rather than just make it a tick the box exercise, feels like the more important question right now.

Ongoing Monitoring and Governance

There is one more dimension worth raising, and it connects directly to what I've observed inside financial institutions: the question of whether ongoing monitoring is actually working.

Tranche 2 entities will need to monitor their clients, flagging who seems suspicious, whether a transaction size feels unusual, whether a client relationship has changed in ways that don't add up. But here's the thing: for most of these businesses, that monitoring will be entirely judgment-based. No system. No calibration. No benchmark. Just whatever the practitioner's experience and instinct tell them on a given day.

That might sound workable. But consider what it takes even for a well-resourced institution to know whether its monitoring is effective. At Tier-2 and Tier-3 banks, with dedicated analytics teams, tuned systems, and established governance, validating whether a monitoring approach is catching what it should routinely takes weeks. Not to find the risk. Just to confirm the mechanism for detecting it is functioning as intended.

A small accounting firm has none of that. No baseline to compare against. No team to sense-check the output. No way of knowing if their judgment is well calibrated or quietly missing things. The obligation is genuine. The capacity to know whether you're meeting it meaningfully is not.

The Work That Follows

I have seen financial crime compliance transform from a back-office function to a board-level priority at major institutions. That shift wasn't driven by legislation alone, it took years of sustained pressure, visible consequences, and genuine operational investment before compliance became part of the culture and embedded across the business.

That same shift needs to happen across newly regulated professions. The legislation is the starting line. What gets built in the years that follow the culture, the habits, the professional norms will determine whether gatekeeper regulation delivers on its promise.

I don't have a clean answer to how that gets accelerated. But after nearly two decades of transformation work inside institutions with resource advantage, I'm confident the question of 'how' matters as much as 'whether'. Right now, it deserves more attention than it's getting.

Sunny Nagpal

FROM GREY-LISTED TO GATEKEEPER: REGULATING PROFESSIONAL SERVICE PROVIDERS AS AML/CTF FRONTLINE ACTORS

LESSONS FROM SOUTH AFRICA

Abraham Ename Minko (PhD) | Senior Researcher and Policy Analyst in Peace, Security and Conflict Resolution, Istanbul University

Introduction

For decades, anti-money laundering and counter-terrorism financing (AML/CTF) regulation focused almost exclusively on banks and formal financial institutions. Yet the architecture of modern financial crime has always extended far beyond them. Lawyers who structure opaque asset transfers, accountants who manage shell companies, real estate agents who execute high-value cash transactions, and trust service providers who engineer complex ownership arrangements are equally attractive to illicit actors — offering the legitimacy of professional standing as a cover for criminal flows. This recognition has driven one of the most consequential shifts in global financial governance: the systematic extension of AML/CTF obligations to Designated Non-Financial Businesses and Professions (DNFBPs).

Globally, this shift is accelerating. Australia's landmark 2024 amendment expanded its framework to lawyers, accountants, and real estate professionals, effective July 2026. The United Kingdom created a single professional services AML/CTF supervisor — the Financial Conduct Authority — in October 2025. The EU's Sixth AML Directive introduced criminal liability for professional 'enablers' of financial crime. In Africa, these trends intersect with distinctive realities: dynamic informal economies, nascent supervisory institutions, and deeply embedded professional self-regulation. South Africa — grey-listed by the Financial Action Task Force (FATF) in October 2023 and removed in February 2025 — offers the continent's most instructive case study of what effective DNFBP reform requires, and what it leaves unresolved.

The Global Architecture of DNFBP Regulation

FATF Standards and Their Uneven Implementation

The DNFBP category entered the FATF Forty Recommendations in 2003, acknowledging that professional service providers — lawyers, accountants, real estate agents, dealers in precious metals, and trust company service providers — occupy strategic nodes in money laundering networks. Their services are not incidental to financial crime; they are often its enabling infrastructure. The FATF framework therefore requires these entities to implement customer due diligence, maintain transaction records, identify politically exposed persons, and file suspicious transaction reports — obligations long familiar to banks, but contested in professions organised around client confidentiality and adversarial legal privilege.

Translation of these standards into national law has been sharply uneven. Jurisdictions have diverged on the scope of coverage, the allocation of supervisory authority between state bodies and professional associations, and the resolution of tensions between disclosure and privilege.

These divergences are not merely technical — they reflect deep disagreements about state authority over learned professions and the relative weight of financial crime prevention in crowded regulatory agendas. The persistent challenge across jurisdictions is not legislative architecture but compliance culture: transforming gatekeeping from a formal box-ticking obligation into a substantive professional commitment.

South Africa: Reform, Enforcement, and Persistent Gaps

Legislative Transformation Since 2022

South Africa's 2022 General Laws Amendment Act introduced sweeping changes to the Financial Intelligence Centre Act (FICA), expanding the universe of 'accountable institutions' to include attorneys, accountants, estate agents, and trust and company service providers. New beneficial ownership registers for companies and trusts created systematic visibility into ultimate control structures for the first time. Crypto asset service providers were formally classified as accountable institutions, with 248 licensed by December 2024 under the Financial Sector Conduct Authority's (FSCA) regime — and subject to the AML 'travel rule' from April 2025. These reforms addressed the core structural deficiencies identified in South Africa's FATF mutual evaluation and provided the legislative foundation for the Financial Intelligence Centre's (FIC) expanded supervisory mandate.

Enforcement Escalation and Structural Compliance Gaps

Legislative reform was accompanied by a marked escalation in enforcement. The FIC, FSCA, South African Reserve Bank, and South Africa Revenue Service (SARS) established coordinated oversight, enabling concurrent scrutiny across regulatory domains. The FIC's 2024/25 reporting records hundreds of inspections, over 3,000 intelligence reports, and asset recoveries exceeding R140 million. The FSCA imposed approximately ZAR 943 million in administrative penalties on 31 individuals in 2023/24 alone — a decisive break from prior supervisory tolerance.

Yet South Africa's National Treasury has acknowledged persistently low DNFBP compliance rates. Regulators repeatedly identify the same deficiencies: inadequate suspicious transaction reporting, insufficient customer due diligence, poor monitoring of politically exposed persons, and the near-absence of automated sanctions screening. Underlying these technical failures is the 'tick-box compliance' phenomenon — policies drafted, registers maintained, certificates issued, but the underlying risk culture unreformed. This reflects structural realities: many DNFBP firms are small, under-resourced, and operating in markets where compliance investment competes directly with service delivery. It also reflects the unresolved tension between FIC supervisory authority and the normative autonomy of professional associations whose members may experience AML obligations as state encroachment rather than shared professional responsibility.

> *'The deepest challenge is not legislative architecture but professional culture — transforming the gatekeeper role from external imposition to intrinsic professional identity. This cannot be legislated into existence; it must be cultivated.'*

Comparative Lessons and the African Regulatory Horizon

What South Africa's Experience Reveals

South Africa's trajectory from grey-listing to re-whitelisting in approximately eighteen months identifies several conditions that appear necessary for successful DNFBP integration: political commitment of sufficient intensity to override professional resistance; a credible, adequately resourced supervisory authority capable of consequential enforcement; and a collaborative framework in which professional associations serve as norm transmitters rather than primary enforcers.

The FIC's deployment of AI and machine learning to enhance intelligence throughput points toward a model particularly relevant for resource-constrained African regulators — leveraging technology to multiply the impact of limited supervisory capacity.

Yet the experience also reveals the limits of rapid reform. Compliance levels achieved under grey-listing pressure may not prove sustainable in its aftermath. South Africa now confronts what other African jurisdictions will eventually face: whether the cultural transformation of professional practice, not merely its formal regulation, can be consolidated and deepened once the external urgency has passed.

Implications for Grey-Listed African States

Algeria, Angola, and Côte d'Ivoire each face FATF pressure to extend and enforce DNFBP obligations, but within institutional environments that differ substantially from South Africa's. Civil law frameworks, varying degrees of state-profession relations, and regional integration dynamics within the West African Economic and Monetary Union (WAEMU) create distinctive regulatory challenges. What these jurisdictions share is a structural vulnerability common across Africa: porous boundaries between formal and informal professional practice, and professional networks that facilitate capital movement across borders in ways that make compliance monitoring technically challenging. An effective African model of DNFBP regulation must adapt FATF standards to these realities — neither dismissing professional self-regulation as irrelevant nor relying on it as a primary enforcement mechanism.

Conclusion

South Africa's reform experience demonstrates that rapid, consequential change in DNFBP regulation is achievable — that political urgency, institutional investment, and international pressure can combine to fundamentally reorient a national AML/CTF architecture. It equally demonstrates that legislation and enforcement escalation are necessary but insufficient. The persistence of 'tick-box compliance' across the legal, accounting, and real estate sectors reveals that durable effectiveness requires the cultural integration of gatekeeping as a professional identity, not merely a regulatory burden.

For Africa's regulatory community, the lesson is both encouraging and sobering. The question is no longer whether professional service providers should be regulated as AML/CTF frontline actors — that question is settled globally and increasingly on the continent. The question is how to make that regulation real: sustained, substantive, and embedded in professional practice rather than performed under the pressure of grey-listing. Addressing that question demands collaborative supervisory architectures, intelligence-led enforcement, investment in regulatory technology, and — above all — a long-term commitment to professional culture transformation that extends well beyond the regulatory cycle.

‘South Africa's experience is a beginning, not an endpoint — a case study that raises as many questions as it resolves, and that invites the sustained, empirically grounded research that this challenge demands across the African continent.‘

Abraham Ename Minko

GATEKEEPERS WITHOUT VISIBILITY: STRUCTURAL LIMITS ON DNFBPS IN DETECTING FINANCIAL CRIME

Nazim Khaja | Compliance and AML/CTF Officer at EFTEX

Calls to regulate lawyers, accountants, real estate professionals and other designated non-financial businesses and professions (DNFBPs) often rest on a simple proposition: if they sit near the movement or structuring of illicit wealth, they should help stop it. The proposition is correct, but incomplete. The deeper failure of DNFBP regulation is not non-compliance. It is the expectation that professions operating with partial visibility can deliver outcomes designed for institutions with full sight of financial behaviour.

The modern anti-money laundering and counter-terrorism financing (AML/CTF) framework was built around institutions with continuous visibility over customer behaviour, transaction flows and account activity. Banks can observe patterns over time, monitor counterparties, identify unusual movement of funds and escalate anomalies using internal intelligence and external reporting channels. Many DNFBPs operate in a fundamentally different environment. They may see a client at a single point in time, for a specific task, with limited access to underlying financial behaviour. Where policy ignores that distinction, obligations become structurally incapable of delivering outcomes.

Why Gatekeepers Matter

This matters because DNFBPs do play an important role in the financial integrity ecosystem. Certain services create genuine control points. Company formation, trust and corporate administration, property transactions, movement of client funds, management of legal structures and professional certification can all be used to create distance between criminal proceeds and their origin. Professional expertise provides legitimacy and access. The same channels can be misused.

The issue is not whether DNFBPs matter. It is whether the model used to regulate them reflects how they actually operate.

Why Bank-Based Models Fail DNFBPs

A recurring weakness in global DNFBP reform has been the tendency to transplant bank-style obligations into sectors with very different operating models.

‘Identical rules do not produce identical outcomes.’

A trust and company service provider establishing complex cross-border structures presents a different risk profile to a suburban accountant preparing tax returns. A casino handling high volumes of cash differs materially from a solicitor engaged for a one-off conveyance. A real estate intermediary may observe unusual purchasing behaviour, but not necessarily the full provenance of wealth behind layered financing arrangements. Treating these activities as equivalent may create legal consistency, but it does not produce regulatory effectiveness.

Visibility is the Real Constraint

DNFBPs are expected to identify patterns they are structurally unable to observe. Many DNFBPs lack long-term customer relationships. A solicitor facilitating a one-off property transaction may rely entirely on client-provided documents, without visibility into the upstream source of funds or broader transaction chain. Similarly, an accountant may structure a multi-jurisdictional entity arrangement based on client instructions. How funds move through those structures often sits outside their view. Once the transaction is completed, visibility often ends. They may sit outside payment rails altogether.

Beneficial ownership data often remains fragmented across jurisdictions. Complex structures may involve multiple advisers, nominee arrangements or offshore entities, each holding only part of the picture. No single professional may possess sufficient information to identify the full risk narrative. You cannot detect what you cannot see. This constraint is not unique to DNFBPs. It reflects how the broader financial crime framework itself is constructed. Where information is partial, fragmented or discontinuous, the system does not fail at the margins — it is constrained at its core. This does not mean DNFBPs should be exempt from obligations. It means obligations should be anchored to realistic access to information. DNFBPs are not failing to detect financial crime. They are being asked to detect what the system itself does not allow them to see.

Why DNFBP Regimes Underperform in Practice

Where DNFBP regimes underperform, the cause is not always resistance from industry. Frequently, it is a weak implementation ecosystem. International assessments have repeatedly identified low awareness of ML/TF risk, poor understanding of obligations, weak sector guidance, under-resourced supervisors and limited outreach. In those settings, low reporting volumes are often interpreted as indifference when they may instead reflect uncertainty, poor calibration or lack of confidence in what constitutes a reportable suspicion.

What appears as non-compliance is often a function of structural limitation. A system that measures success by the volume of forms submitted will create noise. A system that fails to differentiate between sectors will overburden low-risk actors while missing higher-risk activities. Regulation by headline is easy. Regulation by design is harder.

There are better models emerging. Some jurisdictions have recognised that effective DNFBP reform requires more than legislation. It requires sustained engagement between regulators, supervisors, financial intelligence units and the professions themselves. Clear typologies, practical examples, feedback loops, sector-specific guidance and lawful information-sharing channels can materially improve outcomes. The objective should not be more reporting for its own sake, but more accurate, complete and actionable intelligence.

Australia’s Tranche 2 Opportunity

Three design principles should guide the next phase of reform. First, move from title-based regulation to activity-based regulation wherever possible. The relevant unit of risk is often the service being performed, not the profession named on the letterhead. Incorporating a shell company, managing client funds, establishing opaque ownership chains or facilitating high-value transactions may justify stronger controls than low-risk advisory work with no movement of value.

Second, align obligations to visibility, recognising that visibility is uneven and often fragmented across DNFBP sectors and activities. Where a sector can reasonably identify source of funds indicators, beneficial ownership anomalies or suspicious transactional behaviour, expectations should be higher. Where visibility is inherently limited, obligations should focus on gateway controls: identity verification, understanding purpose, escalating red flags, refusing suspicious engagements and preserving records.

Third, judge effectiveness by outcomes rather than formal coverage. Better measures include supervisory capability, quality of suspicious matter reporting, use of intelligence, targeted interventions in high-risk sectors, remediation of known weaknesses and evidence that criminals face greater friction when attempting to exploit professional services.

Australia now has a narrow but significant opportunity as Tranche 2 reforms progress. The temptation in any reform cycle is to replicate established overseas DNFBP frameworks, particularly those seen in the United Kingdom and European Union, and claim alignment with international standards. That would be a missed opportunity.

More effective reform requires selective adoption, not replication. Mature regimes offer useful components: the United Kingdom's depth of sector-specific guidance, the European Union's legislative coverage across professional services, and more centralised supervisory approaches seen in jurisdictions such as Singapore and Hong Kong. But these systems also reveal persistent limitations, including fragmented supervision, uneven implementation and ongoing visibility constraints. Some countries have sought to structure relationships with the private sector to enhance information-sharing and develop strategic and operational intelligence. This includes formalised public–private partnerships (PPPs) and ongoing strategic dialogue with financial institutions and DNFBPs. Such frameworks support financial investigations, asset tracing and financial crime litigation, while enabling the exchange of red flag indicators, emerging risk insights and feedback on suspicious transaction reporting.

'This is where reform must shift from imposing obligations to enabling capability. Structured public-private engagement is not a supplementary feature of effective AML systems — it is central to them.'

In the Australian context, this creates a clear pathway to deepen coordination not only with AUSTRAC, but across law enforcement and asset recovery bodies such as the NSW Crime Commission. Where DNFBPs operate with partial visibility, system effectiveness depends on how well that fragmented information is brought together, analysed and acted upon. Australia can build a more mature framework from the outset: one that recognises sector diversity, calibrates obligations to genuine risk exposure, strengthens beneficial ownership transparency, invests in practical guidance and supports supervisors to engage intelligently rather than mechanically.

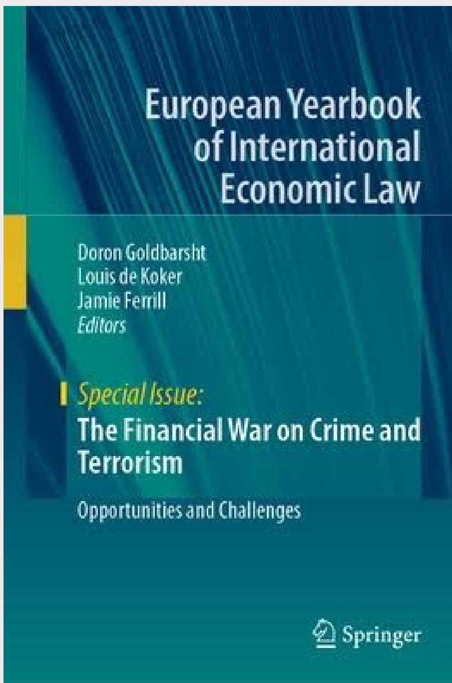
The professions should also view this moment strategically. Regulation assumes visibility, but practice does not. Well-designed gatekeeper obligations are not merely a compliance burden. They are part of the institutional trust architecture that underpins open markets. Professions that can demonstrate proportionate controls, ethical resilience and credible escalation pathways strengthen their own legitimacy.

Gatekeepers matter. But gatekeepers without visibility cannot carry the same expectations as institutions with full sight of financial behaviour. DNFBP reform will not succeed by expanding obligations. It will succeed by recognising the structural limits of visibility and designing a system that works with them, rather than against them.

Nazim Khaja

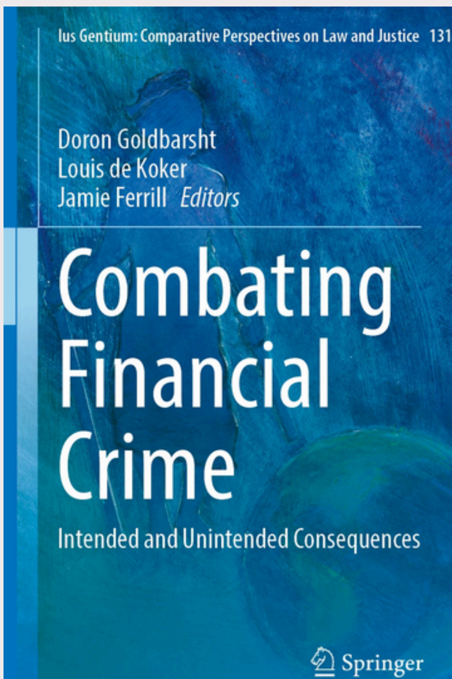
RESEARCH AT FIH

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



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

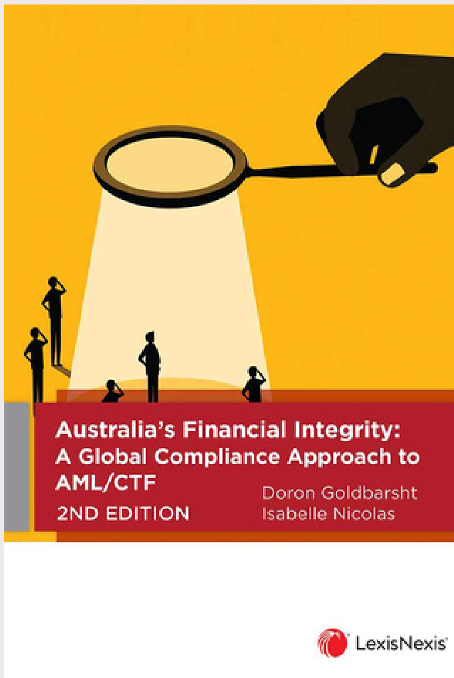
COMBATING FINANCIAL CRIME: INTENDED AND UNINTENDED CONSEQUENCES (2026)



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

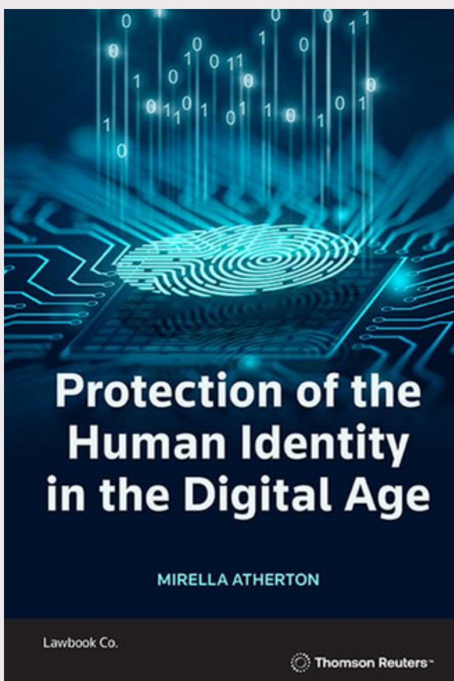
RESEARCH AT FIH

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



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

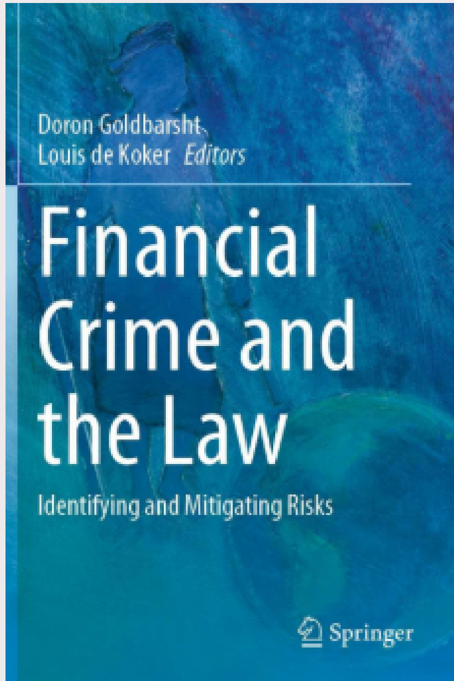
PROTECTION OF THE HUMAN IDENTITY IN THE DIGITAL AGE (2025)



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

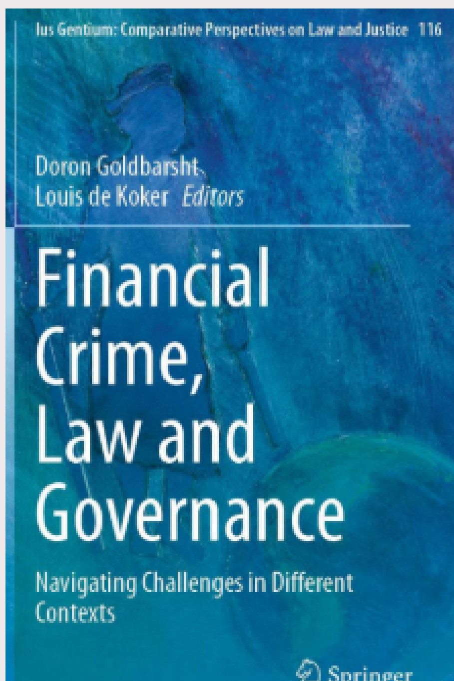
RESEARCH AT FIH

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



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)

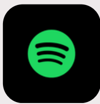


Edited by Doron Goldbarsht and Louis De Koker, this collection was curated by leading researchers to explore the dynamic landscape of global financial crime. It offers profound insights into the nuanced world of financial crime across diverse jurisdictions including Australia, Germany, New Zealand, Nigeria 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.

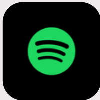
FIH PODCAST

Listen to us on Spotify!
Season 3 of the *Financial Integrity Hub* Podcast

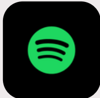
The Financial Integrity Hub hosts regular podcasts, featuring speakers with financial crime and compliance expertise. Each episode involves an interview with a global or local expert, allowing the Financial Integrity Hub to harness critical voices and ensure the Financial Crime community can stay up-to-date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



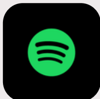
Episode 1 – Payment Systems and Financial Crime, with Toby Evans



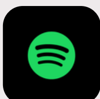
Episode 2 – Anti-Money Laundering and Asset Recovery, with Jeffrey Simser



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



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



NEW! Episode 5

In the latest FIH Podcast episode, Dr Hannah Harris is joined by David Lewis, former Executive Secretary of the Financial Action Task Force (FATF) and a leading voice on anti-money laundering, counter-terrorist financing, and illicit finance policy and practice, for an in-depth discussion on the future of AML/CTF regulation and the importance of shifting the focus of evaluation frameworks toward a more practically grounded assessment of risk, impact, and effectiveness.

Thank you to our podcast partner – Arctic Intelligence!

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

FIH FINANCIAL INTEGRITY WEEK 2026

EXCELLENCE, TRANSPARENCY & LEADERSHIP

In May 2026, the **Financial Integrity Hub** hosted the first Financial Integrity Week event, a premiere three-day event bringing together leading voices from academia, government, and the private sector to address the most pressing challenges in financial crime and regulatory integrity. Co-hosted with the **Australian Transactions Reports and Analysis Centre (AUSTRAC)** and the **Australian Federal Police (AFP),** the program featured high-level panels, expert seminars, and curated networking opportunities designed to foster meaningful dialogue and collaboration across sectors.

Image: 2026 *Financial Integrity Week*.

PREVIOUS EDITIONS

Countering Terrorist Financing and Violent Extremism
March 26 Edition

Financial Crime and Technology
December 25 Edition

Sanctions
September 25 Edition

Virtual Assets & Virtual Asset Service Providers
June 25 Edition

Information Sharing
March 25 Edition

AML/CTF Reform Implementation
December 24 Edition

National Risk Assessment
September 24 Edition

WORK WITH US

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

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

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

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

FINANCIAL INTEGRITY HUB

MACQUARIE University SYDNEY·AUSTRALIA

Thank you to our partners for their support!

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

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!