THE INTERNATIONAL ACADEMY
OF FINANCIAL CRIME LITIGATORS

Bulletin

of The International Academy of Financial Crime Litigators

ISSUE 6 | SPRING 2026

Bulletin of The International Academy of Financial Crime Litigators

Paris, France

Editors: Jonathan S. Sack and Maria Nizzero

Editorial Board/Publishers: Stéphane Bonifassi, Lincoln Caylor and Elizabeth Ortega

Publication/Art Director: ECO Strategic Communications

The Bulletin appears twice a year and is available free of charge.

Current and back issues are available online at:
https://financialcrimelitigators.org/publications/

To sign up for a subscription or to report an address change please send an email to contact@financialcrimelitigators.org.

For editorial comments or inquiries, please contact the editors at jsack@maglaw.com and maria.nizzero@ukfinance.org.uk or at the address below.

For further information about The Academy, please visit our website www.financialcrimelitigators.org.

For general inquiries, please send an email to contact@financialcrimelitigators.org.

ISSN 2999-3938

Contents

ISSUE 6 | SPRING 2026

Letter FROM THE EDITORS

Inspired by Women International Day, this issue of the Bulletin sought to reflect the growing presence of women lawyers in leadership by featuring an all-women lineup of contributors in financial crime. Across the four contributions gathered here, the authors provide fresh perspectives on criminal procedure, fraud, enforcement and related areas with a focus on analysis and practical insight.

The issue opens with a timely examination by **Isadora Fingermann*** of the U.S. Government's use of Foreign Terrorist Organization designations against Brazilian criminal groups, a development that sits at the intersection of extraterritorial enforcement, geopolitical leverage, and corporate compliance risk. Isadora's article offers a lucid account of how a tool designed for ideologically motivated terrorism is being repurposed against purely criminal organizations, and what that means for firms operating in one of Latin America's largest economies.

Sue Thackeray* follows with her analysis of the UK Government's new Fraud Strategy. The article describes a framework that reflects a more detailed understanding of the risks and systemic conditions that enable one of the most harmful economic crimes in the UK. It also pressures government in focusing on implementation, and provides a series of practical recommendations for practitioners, particularly with regards to the review of their compliance frameworks in light of the failure-to-prevent offence.

Karyn Harty's* contribution turns to Ireland's asset forfeiture regime and provides a thorough analysis on a topic already touched in previous Bulletin's issues: the concept of unexplained wealth. Her account of the Criminal Assets Bureau's recent breakthrough in accessing encrypted Bitcoin reads as a striking illustration of the article's central thesis that the ease or difficulty of enforcement inevitably influences which assets are ultimately seized.

The issue closes with a Q&A featuring **Professor Karen Woody***, whose responses to five questions by our one and only **Elizabeth Ortega*** on insider trading risks in Big Law offer some food for thought on a compliance landscape that is, as she puts it, unstable by any objective measure.

The four contributions speak to one another in ways their authors may not have planned. All four grapple, in different registers, with the same underlying problem: that enforcement frameworks built for a simpler world are straining under the weight of financial crime that is global, technologically sophisticated, and structurally embedded in legitimate economic activity. The response, whether in the form of FTO designation, civil forfeiture, policy reform, or compliance architecture, inevitably brings into question matters of institutional design, political will, and the values that the legal system chooses to prioritize.

It is a particular pleasure to publish this issue under the banner of "Women of the Academy." The quality of the work here speaks for itself. But it is worth marking, plainly, that the perspectives gathered in these pages represent exactly the kind of scholarship and practice that the field needs more of, and that the International Academy of Financial Crime Litigators seeks to promote. We are grateful to each of our contributors, and we commend this issue to you.

** Fellows of The Academy*

We hope you enjoy this issue of
The Academy Bulletin.

Jonathan S. Sack* | *Editor*

Maria Nizzero* | *Editor*

The Designation of Brazilian Criminal Organizations as Foreign Terrorist Organizations (FTOs) by the U.S. Government: Legal Consequences in Brazil.

ISADORA FINGERMANN

This article outlines the critical aspects surrounding the potential classification of Brazilian criminal organizations as Foreign Terrorist Organizations (FTOs), emphasizing the need for new and enhanced preventive and compliance measures within companies to mitigate criminal and civil liability in both Brazil and the United States, particularly concerning anti-money laundering initiatives within the financial sector.

Introduction

In the context of increasingly complex and strained international relations, the focus of criminal law and law enforcement authorities is rapidly shifting. Over the past decade, anti-corruption enforcement and anti-money laundering (AML) efforts have developed in parallel as pillars of international criminal policy – the former significantly propelled by the U.S. Foreign Corrupt Practices Act (FCPA) and the related anti-corruption laws enacted globally in its wake, the latter anchored in the Financial Action Task Force (FATF) recommendations and successive waves of national AML legislation. The coming years, however, herald the intensification of enforcement of AML on the financial dimension of predicate offences to money laundering, with particular emphasis on the flow of funds originating from drug and arms trafficking, which frequently finance abhorrent terrorist activities.

As the focus of international criminal policy transitions from traditional crime, such as drug trafficking and terrorism, to the financial flows that underpin and emerge from these activities, and the interactions between illegal and legal economic activities, this issue must take center stage in discussions regarding the criminal, regulatory, and reputational risks faced by major multinational corporations. The convergence of these risks is now being given a sharper legal edge through the more aggressive use of Foreign Terrorist Organizations (FTOs) designations targeting transnational criminal groups.

Brazil offers a particularly compelling case study of this evolving paradigm. The country's two largest criminal organizations – the *Primeiro Comando da Capital* (PCC) and the *Comando Vermelho* (CV) – have long transcended their origins as prison-based groups, developing sophisticated transnational networks deeply embedded in international drug trafficking routes and, increasingly, in legitimate economic sectors such as fuel distribution,

gambling, and financial services. As the United States expands its use of FTO designations beyond ideologically motivated groups to encompass transnational criminal organizations operating in Latin America, the potential classification of the PCC and the CV has emerged as a focal point of legal, political, and diplomatic debate – with far-reaching ramifications for companies operating in or with exposure to the Brazilian market.

UNDERSTANDING FOREIGN TERRORIST ORGANIZATIONS (FTOS).

The designation of FTOs is governed by the U.S. Department of State under Section 219 of the Immigration and Nationality Act (INA). To qualify as an FTO, an organization must meet three criteria: it must be a foreign organization, it must engage in premeditated, politically motivated violence against non-combatant targets, and it must pose a threat to the security of U.S. nationals or national security. This classification carries profound implications, allowing the U.S. government to impose a range of sanctions on the target, including asset freezes, travel bans for members, and restrictions on financial transactions.

The designation of organizations as FTOs is not a new instrument: the U.S. Department of State has maintained an FTO list since 1997, initially targeting politically and ideologically motivated groups, in Latin America and elsewhere. Beginning in early 2025, coinciding with the suspension of FCPA enforcement efforts by the Trump administration, the United States adopted a materially different enforcement posture by, pursuant to Executive Order 14157, extending terrorism-designation tools to drug cartels and transnational criminal organizations (TCOs), such as the classification of various criminal groups operating in Latin American countries as FTOs.

The policy was further operationalized by the Department of Justice's "Total Elimination of Cartels and Transnational Criminal Organizations" memorandum, which specifically directed the FCPA Unit to prioritize foreign-bribery investigations that facilitate Cartels and TCOs operations, and directed the Money Laundering and Asset Recovery Section (MLARS) to prioritize money laundering investigations, prosecutions, and asset forfeiture

actions – highlighting a shift away from traditional FCPA enforcement toward FTO-related matters.

Initial efforts have primarily targeted organizations operating in countries traditionally associated with U.S. foreign policy interventions, such as Mexico, Venezuela, and Colombia. The first eight designations of criminal organizations as FTOs occurred in the first half of 2025, served as a legal predicate for a series of aggressive unilateral measures, including the bombing of Colombian vessels in international waters of the Pacific Ocean, and the January 2026 capture - without congressional approval—of the then-President of Venezuela, Nicolás Maduro, to face narco-terrorism charges in the Southern District of New York.

As a matter of U.S. law, FTO designations have broad compounding effects: they authorize the extraterritorial application of U.S. law; they expand the definition of material support for criminal conduct; they attract the jurisdiction of national security agencies; they facilitate multi-lateral financial sanctions; and allow the executive branch to impose unilateral measures, including asset freezes, without the necessity of prolonged judicial processes in the U.S. or international courts. This intersection of criminal policy efforts with economic interests, extraterritorial political measures, and regional influence efforts is becoming increasingly visible.

FTO DESIGNATIONS OF BRAZILIAN CRIMINAL ORGANIZATIONS.

Brazil, a country of continental scale with a more robust institutional framework than most of its Latin American neighbors, would not appear to be an immediate candidate for U.S. foreign action of the kind recently employed in Venezuela. However, there have been growing discussions surrounding the potential designation of the primary two criminal organizations operating in the country, the *Primeiro Comando da Capital* (PCC) and the *Comando Vermelho* (CV). This move, opposed by the current government, but favored by the opposition – the son of former president Jair Bolsonaro, currently imprisoned and barred from running - raise questions as to whether U.S. extraterritorial action could serve as a tool for interference in the presidential elections of October 2026.

The PCC and CV are long-established Brazilian criminal organizations. The former, larger in size (approximately 40,000 members), was founded in São Paulo in 1993 and is known for its significant international drug trafficking operations, particularly cocaine, to Europe, Asia, and Africa. The latter, slightly smaller (about 25,000 members), originated in Rio de Janeiro in 1979 and has a more limited international footprint, concentrated primarily along the border with Paraguay. Both groups share a common origin in the Brazilian prison system, where they initially emerged to advocate for better prison conditions. Their economic objectives expanded with the high profitability of drug trafficking and, more recently, have shifted to activities involving infiltration of legitimate sectors, including gambling and fuel distribution.

Although Brazil has had a law combating criminal organizations such as the PCC and CV since 2013 (Law No. 12,850/2013), facilitating more invasive investigative measures, international cooperation, and plea bargains, alongside an anti-terrorism law in force since 2016 (Law No. 13.260/2016), neither group can be classified as a terrorist organization as they lack ideological or partisan motivations and do not maintain territorial control comparable to that seen in Mexico or Colombia, for example. This is evidenced by the fact that, despite intense pressure from the U.S. government and Brazilian far-right legislators, the Brazilian Congress rejected the definition of these two groups as terrorist organizations in 2025.

This does not mean that Brazil is inactive in combating organized crime and particularly these two criminal organizations. Quite the contrary, the recent police operation *Carbono Oculto*, launched in August 2025, and resulting in BRL 1.4 billion (USD 280 million) blocked by Brazilian courts, represents the latest of these efforts: it exposed the PCC's involvement in legitimate fuel commerce and the role of financial institutions and investment funds in supporting the complex money laundering structure of these criminal groups.

WHY DOES THIS MATTER?

FTO designations, whether domestic classifications or U.S. led, are unlikely on their own to weaken organized crime in Brazil or hinder international drug trafficking. Both the PCC and CV have repeatedly adapted to pressure

by fragmenting operations, expanding front companies, and moving into opaque financial channels. Other countries where drug gangs have been designated as FTOs – including Mexico, Colombia, and Haiti – have not seen a material decline in violence. The classification, along with its implications, may even accelerate the financial sophistication of these criminal groups, driving transactions through cryptocurrency and trade-based laundering and deepening penetration of legitimate sectors.

In Brazil, the disruptive potential of an FTO designation lies less in its direct impact on the PCC or CV and more in the tools it unlocks against the enabling environment. The PCC alone has been linked to an estimated 52 billion reais ($10 billion) in assets across agribusiness, construction, logistics, and real estate. This designation paired with Office of Foreign Assets Control (OFAC) sanctions would expose any company transacting with a PCC-linked intermediary to U.S. investigations and asset-blocking risk wherever there is a U.S. nexus.

The FTO designation of these criminal organizations, which, at the time of writing, appears to be imminent, may increase litigation and regulatory risks for firms operating in Brazil and in the broader Latin American region. If strategic economic sectors critical to organized crime (e.g., financial institutions, logistics companies, fuel industries, ports, etc.) do not swiftly prepare for this shift in the international law enforcement landscape by implementing effective preventive measures, they may endure significant legal and reputational consequences stemming from the transformation of the PCC and CV into FTOs.

Criminal organizations of the size and economic significance of the PCC and CV do not operate dissociated from the financial system or isolated from legitimate economic activities. Criminal groups—whether classified as FTOs or not—engage through or in concert with formally established companies, including those that may be part of supply chains for inputs or services, logistics, technology, or the marketing of various products unrelated to narcotics, such as the fuel trade in Brazil. Companies across all sectors—including retail and digital platforms—may inadvertently maintain direct or indirect relationships with structures linked to organized crime, facilitating or even enabling their activities. The FTO designation would amplify the legal exposure of any company – domestic or foreign – found to have even an indirect nexus with

the designated organization. Under 18 U.S.C. § 2339B, it is a federal crime to knowingly provide "material support or resources" to a designated FTO – a prohibition carrying penalties of up to twenty years of imprisonment per count, or life imprisonment if a death results from the conduct.

The statute defines "material support" in extraordinarily broad terms: it encompasses not only funds and financial services, but also lodging, transportation, personnel, training, expert advice or assistance, communications equipment, and any other tangible or intangible property. This means that routine commercial transactions – payments to suppliers in territories where FTO-designated groups exert influence, the engagement of logistics providers with ties to designated organizations, or even the unwitting provision of financial services that benefit an FTO – could trigger federal criminal liability in the U.S.

This scenario may also prompt investigations in Brazil for involvement in criminal organizations (Section 2nd, Law No. 12.850/2013) or for money laundering (Section 1st, Law No. 9.613/1998). Since Brazilian law does not impose criminal liability on legal entities (except for environmental crimes), criminal responsibility will fall on individuals who participated in or permitted the potentially criminal activity within the company's operations. However, criminal investigations related to money laundering and involvement in organized crime are generally associated with the imposition of precautionary measures against companies, such as searches and seizures and assets or fund freezes, alongside severe reputational consequences.

Depending on the nature of the relationship, the crime of corruption may also be present. Companies interacting with third parties (i.e., distributors, business partners, suppliers, payment institutions, etc.) must exercise heightened vigilance in their activities, as integrity risk should be treated as a core business risk, not confined to sectors traditionally associated with illegalities. Companies are held accountable for harmful acts committed in their interest or benefit, even if perpetrated by third parties, and failures in this regard may result in serious liability under the Brazilian Anti-Corruption Law (Law No. 12,846/2013), with financial sanctions potentially reaching 20% of the company's gross revenue from the year preceding the misconduct, forfeiture of assets, rights, or values representing advantages or benefits obtained directly or indirectly from the violation, and prohibition from

receiving incentives, subsidies, grants, or public loans—regardless of the company's knowledge or consent.

In cases of interaction—direct or indirect—with FTOs, the consequences for financial institutions or companies may be even more severe. A legal entity present in a territory dominated by an FTO, or that hires a security company with ties to an FTO, or that make a payment to expedite cargo release at a FTO-controlled port, or even that have subcontractors with such kind of interactions may face repercussions such as asset freezes, suspension of SWIFT access, embargos, and other substantial consequences.

CONCLUSION

The extraterritorial application of U.S. jurisdiction to address criminal organizations unilaterally designated as Foreign Terrorist Organizations (FTOs) appears to be a growing trend. Consequently, business groups that proactively strengthen preventive measures to mitigate interactions with these organizations will gain a competitive edge in safeguarding their operations and reputations.

Companies must extend their tracking of financial flows related to goods and services, meticulously mapping and monitoring supply chains from origin and importation through processing, distribution, and delivery to the end consumer. It is vital for companies to enhance financial systems and high-risk payment channels, enforcing robust Know Your Customer (KYC) procedures for intermediaries and monitoring transaction patterns (e.g., excessive cash usage, unusual transaction linkages). Companies must also ensure absolute clarity when transactions are conducted in U.S. dollars or in any manner that intersects with the U.S. financial system.

Moreover, companies need to guarantee transparency in their investment and ownership structures by verifying ultimate beneficial owners, requiring independent assessments, and maintaining ongoing monitoring for sanctions and negative media exposure. Additionally, businesses should reinforce anti-corruption controls in their interactions with government entities, implement rigorous due diligence on third parties, establish clear policies on gifts and hospitality, require conflict of interest disclosures, and maintain accurate books and records.

Furthermore, companies must conduct real-time screening of counterparts and intermediaries against U.S. Office of Foreign Assets Control (OFAC) lists and other relevant lists, incorporating contractual clauses that allow for termination if entities become sanctioned or linked to criminal organizations. Finally, but equally importantly, businesses should be prepared for investigations of irregularities, ensuring protection for whistleblowers (e.g., anonymous reporting channels and effective retaliation safeguards), establishing clear processes for addressing warning signs, preserving evidence, and conducting independent reviews.

The era when criminal organizations solely engaged in illicit activities, thus remaining distant from the daily operations of legitimate businesses, is long gone. Criminal groups, whether classified as FTOs or not, are increasingly embedded within regular economic activities, posing criminal, regulatory, and reputational risks to companies that inadvertently engage with them, especially for the financial system. This reality necessitates heightened attention and vigilance from corporate legal teams.

The central concern raised by the potential FTO designation of Brazilian criminal organizations is twofold. First, it represents the deployment of a foreign policy instrument – originally designed for ideologically-motivated terrorist groups – as a tool of extraterritorial criminal enforcement against transnational organized crime. This shift is not merely technical: it expands the jurisdictional reach of U.S. authorities, activates national security apparatus and resources, and creates a legal predicate for unilateral executive action that bypasses traditional judicial and diplomatic channels. In the Brazilian context, the timing of these discussions – coinciding with the October 2026 presidential elections and supported primarily by opposition figures aligned with former President Bolsonaro – raises legitimate questions about whether criminal enforcement objectives are being instrumentalized to serve geopolitical and domestic political interests.

Second, and of more immediate practical consequence for the private sector, the FTO designation fundamentally alters the liability landscape for companies operating in or connected to Brazil. Under existing frameworks, firms are already subject to anti-money laundering obligations and must conduct due diligence to avoid facilitating the proceeds of organized crime. However, this classification introduces an additional and distinct layer of exposure: the

prohibition on material support under 18 U.S.C. § 2339B, which carries criminal penalties of up to 20 years' imprisonment and applies extraterritorially to any transaction with a U.S. nexus. Unlike traditional AML obligations, which require knowledge or willful blindness regarding the illicit origin of funds, the material support prohibition attaches strict liability to any provision of resources to a designated organization, irrespective of the provider's knowledge of the organization's involvement. This expansion of liability means that companies with even attenuated connections to FTO-linked entities through supply chains, payment systems, or commercial relationships may face criminal exposure in U.S. courts, asset freezes under OFAC regulations, and exclusion from the U.S. financial system – consequences that far exceed those associated with conventional AML enforcement.

The potential designation of Brazilian criminal organizations as Foreign Terrorist Organizations by the U.S. government raises intricate legal and political questions. While the implications for U.S. law enforcement and international relations are significant, the consequences within Brazil could be equally profound, impacting legal frameworks, public perception, and the overall security landscape. As these discussions evolve, it is crucial to adopt a nuanced approach that acknowledges the socio-economic factors contributing to the rise of these organizations while navigating the complexities of international law and cooperation.

AUTHOR

Isadora Fingermann is a partner at TozziniFreire Advogados. Head of the White-Collar Crime Practice and member of the firm's Board. Master's degree in policy management (MPM) from Georgetown University. Specialist in White-Collar Crimes at Fundação Getúlio Vargas (FGV/SP). Law degree from the University of São Paulo. Member of the Board of Brazilian Institute of Defense of the Right to Defense (IDDD). Fellow at the Academy of Financial Crime Litigators.

The UK Government's New Fraud Strategy: Key Implications for Enforcement and Compliance.

SUE THACKERAY

Introduction

In March 2026 the UK Government launched the Fraud Strategy 2026-2029, which introduces a new landscape for tackling fraud. Fraud is now the largest type of crime in the UK, costing the economy an estimated £14.4 billion in 2023-2024. The Government recognises that fraud is a crime with significant consequences for both victims and the broader economy, and the new Fraud Strategy is a positive step towards tackling the problem. The core ideas are to improve data sharing, block more online crime at source, and create more resilient industry processes in vulnerable sectors.

In my view, it is a credible strategy that reflects a detailed understanding of the risks and the systems that contribute to fraud in the UK. It builds on the systems set out in legislation such as the Economic Crime and Corporate Transparency Act 2023, which introduced corporate criminal liability for failure to prevent fraud in England & Wales. Now it all comes down to the implementation. This article examines the strategy's key pillars and explores the practical implications for financial crime practitioners, including the increased dependence on civil remedies.

PROBLEMS WITH THE UK'S CURRENT APPROACH TO FRAUD

The Government's approach to fraud has historically suffered from a lack of information sharing between public bodies. This has meant that the fraud response has always been reactive and focused on the post-event investigation rather than targeting the underlying systems that enable fraud in the first place.

The Government has focused on criminal justice, but the system has not been able to achieve sufficient prosecutions to act as a real deterrent. The problem has only been getting worse, with the rise of tech-enabled fraud and AI-driven threats making it harder for the public to detect fraud. Fraud has become a low risk and profitable crime, which has allowed it to become so pervasive.

Financial crime lawyers have long argued that tackling fraud effectively requires a broader toolkit, including greater reliance on the private sector and the use of civil sanctions and enforcement mechanisms alongside traditional criminal justice approaches.

THE NEW APPROACH

The new fraud strategy focuses on three key strands: (i) disrupt (ii) safeguard and (iii) respond. The emphasis is clearly on the "disrupt" pillar, which represents a welcome departure from the traditional reactive model.

(i) Disrupt

The Government is notably shifting its approach to focus on disrupting the systems exploited by criminals to make fraud possible in the first place. It requires a proactive approach, acting early to deny criminals access to the systems they exploit and the profits of their crime.

The flagship announcement is the launch of a new Online Crime Centre. This is a £31 million public-private sector partnership intended to bring together various bodies including the Home Office, the NCA, the police, the intelligence community and private sector partners from the financial, telecoms, technology and cyber industries. It aims to share data and intelligence much more quickly and collaborate on interventions that can identify and intercept online fraud and cyber-crime at scale. The idea is to design technical solutions that support industry to put in place controls and processes early, reducing vulnerability and denying criminal access to the systems that they have historically exploited, and therefore the proceeds of their crime. The strategy also focusses on collaborating with the private sector to deliver interventions that address their vulnerability to fraud; in particular in telecoms, online and financial services. The attempt to address unauthorised fraud in the financial services sector is of particular interest. Since 2024, UK banks have been required to reimburse losses up to £85,000 for APP fraud (where victims are deceived into willingly transferring money). This was perhaps a missed opportunity, as this figure was reduced from the much more meaningful £415,000 due to lobbying from the banking sector, and has not incentivised the banks to take proactive steps to prevent the fraud in the first place. Whilst any reimbursement scheme is still useful, it is an example of the Government's

focus on fixing the outcome of fraud, rather than disrupting the cause of the problem. The Fraud Strategy acknowledges this by launching a call for evidence to assess the scale, drivers and enablers of unauthorised fraud. The Financial Conduct Authority (FCA) also plans to share recommendations for preventing APP fraud with the financial services sector.

The imminent changes to the cryptoasset firm landscape are another positive systemwide development. A new regime comes into force in October 2027 which will mean that cryptoasset firms will need to be authorised by the FCA and to comply with its rules. Activities such as operating a cryptoasset trading platform in the UK will become regulated activities. This is a significant change that means that cryptoasset firms must obtain authorisation, maintain governance and risk management systems and implement robust anti-money laundering controls. The FCA expects firms to be able to monitor transactions and block transactions to high-risk wallet addresses. This degree of regulation should make it easier for victims of fraud to trace cryptoassets, a notoriously difficult area.

(ii) Safeguard

The "Safeguard" pillar focuses on protecting individuals and businesses by providing clearer guidance and more support for vulnerable groups. This should improve public and business resilience to fraud.

It includes the expansion of a national campaign called "Stop! Think Fraud", to raise public awareness and resilience to fraud. It also focuses on support for high-risk sectors and engagement with the private sector on issues such as identity verification.

(iii) Respond

This pillar looks to improve on reporting, investigation and victim care. The City of London has just launched a new Fraud Report service, which replaces Action Fraud as our national platform for reporting cybercrime and fraud. We are supportive of the idea of a centralised fraud reporting system, but Action Fraud was clearly not fit for purpose. In practice, clients were reporting fraud to Action Fraud simply to obtain a reference number for insurance purposes, rather than with any expectation that Action Fraud would assist their case. We hope that Fraud Report can provide a faster response and better recovery outcomes. However, we would also like to see the Government make good use of the critical data that Fraud Report will collect (see further below).

WILL THE STRATEGY WORK?

There is a general consensus that the Fraud Strategy is a positive step in the right direction. However, the implementation will be key and there are some important factors that the Government must focus on.

1. Further investment

The Government is committing to investing over £250 million in fraud prevention and response measures by 2029. This is a welcome announcement and demonstrates that there is real political will to address the problem, but it still pales in comparison to the magnitude of the problem and the economic impact. The scale of the issue will necessitate further investment and commitment to tackle fraud beyond 2029 as well.

The Fraud Strategy references the need to future-proof against emerging technology, deepfakes, stablecoins, blockchain and new payment methods. The next wave of payment innovation and the fraud risks it creates will only offer fraudsters more opportunities to exploit the system. We therefore need to ensure that our response is dynamic, and able to adapt to a changing landscape. This will inevitably require further investment.

2. Successful implementation

One of the most positive aspects of the new strategy is the recognition that fraud is a systemic, industrialised issue. For example, fraudsters have been able to exploit loopholes by creating fake companies or impersonating businesses. A particular problem that we regularly see in practice is criminals intercepting legitimate emails and sending fake invoices. The Fraud Strategy introduces mandatory electronic invoicing for VAT invoices from April 2029, which is a positive initiative that should allow suppliers to generate and send invoices through secure digital systems. However, the Government must ensure that the implementation of this is successful through a well-resourced information campaign. The infrastructure must also be impenetrable, to avoid simply creating another system that fraudsters can exploit.

3. International outlook

The Fraud Strategy also correctly identifies that fraud is a cross-border problem that requires an international outlook. The Government says that

it will pursue more partnerships with high-priority countries, like it has done with Nigeria and Vietnam. Continuing to invest in global research and skills development will be critical to long-term resilience, as fraudsters often operate overseas and target the UK from jurisdictions that are outside of our regulatory framework.

4. Reliance on civil remedies

The Fraud Strategy states that the Home Office is supporting law enforcement pilots focused on pursuing legal action against criminals and recovering money for victims through civil law by 2028. It is also considering introducing civil penalties for fraud and facilitating money laundering as an alternative to the criminal law.

This follows, for example, the introduction of civil penalties in tax fraud by HMRC. The lower burden of proof required under the civil standard in England & Wales would also potentially help with some of the evidential challenges that characterise complex criminal fraud trials.

However, the Fraud Strategy does not contain any detail on what the proposals for civil recovery might look like, or how they would be resourced. Within public bodies, there is a lack of staff with capacity and ability to pursue civil remedies and they have understandably focused on criminal recovery. One of the problems with the traditional civil fraud remedies is that the amount of money that has been lost by an individual or a single business is often not sufficient to justify the expense of recovering it. This is particularly true where individuals or businesses have just been defrauded and may not have the resources to spend further money on a civil claim.

However, fraudsters often target multiple people with the same fraud. If victims were able to find each other, then they could form a collective group and litigate much more effectively. The Report Fraud database is a key repository of this information. The Government should consider the viability of a scheme whereby they (i) analyse the crimes being logged via Report Fraud and (ii) identify groups of victims of the same crime. The Government could then work with external law firms who specialise in financial crime (with criminal and civil expertise) to assess whether a group of victims could make a successful claim for recovery in the civil courts, which could also be funded by alternative fee arrangements or third party funders to reduce or

eliminate up front cost to the individual victims who might have lost their life savings to fraud. This proposal would clearly involve challenges, including in relation to volume and data-sharing, but is worth exploring as an additional tool in the response to fraud.

CONCLUSION

This Fraud Strategy has been long in the making, and its ambition is to be welcomed. The recognition that fraud is a systemic, industrialized problem represents a shift in the Government's thinking. The three-pillar framework of disrupt, safeguard and respond provides a coherent architecture for the strategy. However, the detail and implementation will be critical. The Government must ensure it focusses on the areas outlined above in particular if this strategy is to be a success. In addition, the international dimension cannot be overstated. A domestic strategy can only be effective if it is supported by international partnerships and it is vital that public bodies and lawyers continue to engage across borders to assess new risks as they develop.

For practitioners advising clients on fraud risk and recovery, there are several key priorities. Organizations must review their compliance frameworks in light of the failure to prevent fraud offence, ensuring that adequate procedures are in place and documented, as scrutiny will only increase because of this strategy. Secondly, firms operating in the financial services sector should engage closely with the new regulations, ensuring that they fully understand the requirements. Thirdly, practitioners advising victims of fraud should monitor the development of the civil recovery pilots. The potential for group litigation, potentially facilitated by data from the new Report Fraud platform, could represent a significant new avenue for recovery.

AUTHOR

Sue Thackeray is a partner at Kingsley Napley LLP in London. She is a highly experienced commercial litigator who is widely sought after for her strategic expertise in civil fraud and asset recovery cases, often where criminal proceedings co-exist.

Unexplained Wealth Orders and the Logic of Asset Forfeiture

KARYN HARTY

SHORT ABSTRACT

Asset forfeiture is a central tool in modern law enforcement strategies aimed at disrupting criminal activity by targeting its economic foundations. In Ireland, the forfeiture regime enables the recovery of assets without a criminal conviction in certain circumstances and should be a powerful mechanism for tackling organized crime. A more revealing lens through which to assess its operation, however, is the concept of "unexplained wealth" and the role that evidential constraints and the relative ease of enforcement play in shaping asset forfeiture.

This article argues that asset forfeiture is not a neutral mechanism that simply tracks and penalizes underlying criminality. It is shaped by what can be proven, not necessarily by what is most harmful, which may constrain its impact on organized crime. Focusing on Ireland's model of forfeiture, which explicitly targets unexplained wealth for which a lawful origin cannot be established, this article suggests that the relative and evolving ease or difficulty of enforcement and the location of assets significantly influence which assets are ultimately seized.

THE IRISH MODEL: CIVIL RECOVERY AND THE CENTRALITY OF UNEXPLAINED WEALTH

Ireland's asset forfeiture regime is anchored in the Proceeds of Crime Acts 1996–2016 and is administered primarily through the Criminal Assets Bureau (CAB). CAB is a multi-agency body combining law enforcement, tax, and social welfare functions. It is a highly effective agency whose mandate is not to prosecute criminal offences but to identify and pursue unexplained wealth and deprive individuals of assets derived from criminal conduct. It works closely with An Garda Síochána and other agencies, such as the Revenue Commissioners, to identify and target proceeds of crime.

A defining feature of the Irish system is its reliance on civil proceedings before the High Court, operating on the balance of probabilities rather than the criminal standard of proof. This allows CAB to target assets where criminal prosecution may be infeasible due to evidential limitations. The forfeiture regime enables CAB to seek orders to freeze and ultimately seize and recover assets believed to be the proceeds of crime without requiring a prior conviction.

CAB's establishment marked a deliberate shift away from conviction-based enforcement to a model grounded in financial disproportionality, reflecting a recognition that in many cases, particularly in organized crime, proving specific criminality may be far more difficult than demonstrating that wealth is unjustified. Although Irish law does not formally employ the term "unexplained wealth," the concept is functionally central to how the forfeiture system operates. CAB cases often involve situations where an individual's assets are demonstrably disproportionate to their known lawful income, and the court is invited to infer that the assets derive from criminal conduct unless a credible lawful explanation is provided. Having successfully applied for orders freezing the assets, there is a mechanism for those affected to apply to set aside the orders by demonstrating that they are lawfully held, and CAB must wait seven years before the assets can be forfeited. This extended period of restraint has reflected the constitutional protection of property rights, balanced against the lower civil standard of proof that underpins the forfeiture regime.

There has therefore been a tension between efficiency and personal rights in the Irish model, in that a system that relies on unexplained wealth and civil standards of proof may raise due process concerns, particularly where individuals are required to account for their assets in the absence of a criminal conviction.

WHAT HAPPENS TO RECOVERED ASSETS: A STATE-CENTERED MODEL

An important structural feature of the Irish system is that assets forfeited under the Proceeds of Crime Acts are paid into the Central Fund of the State, effectively becoming part of the general Exchequer. The system is not designed to compensate or return assets to victims of crime.

Forfeiture in Ireland is therefore best understood as a public law tool aimed at depriving criminals of illicit wealth and reinforcing the integrity of the legal and economic system. The result is a highly centralized model in which forfeited assets serve the public good rather than being returned to those impacted by the conduct of the subject of the forfeiture. This feature of the Irish system places it, and other common law jurisdictions which similarly

return forfeited assets to the public purse, in contrast to the system in the United States, which incorporates mechanisms for victim compensation through remission and restoration procedures administered by the Department of Justice. This concept of returning forfeited assets to those affected is not a feature of the Irish model but the public benefits from an increase in exchequer funds.

THE TAX DIMENSION

Drilling down into individual cases, the nature of the assets that CAB tends to recover is revealing. A substantial proportion of CAB's activity involves pursuing individuals for tax liabilities arising from unexplained income. CAB has power to tax all sources of income and can raise tax assessments, issue tax demands and collect unpaid tax. CAB also has the ability to implement all Customs controls and legislation when necessary. For example, more than €13m in recoveries made in 2024 arose from tax assessments.

At first glance, in the context of the growing problem of largescale fraud, a focus on unpaid taxes may appear to reflect a form of mission drift. However, a closer analysis suggests that it is more accurately understood as deriving from the system's underlying logic. Tax law provides a robust and accessible evidential framework for challenging unexplained wealth. Where it is difficult to obtain direct proof of criminal activity, discrepancies in declared income can serve as a basis for intervention that is significantly easier to establish.

The prominence of tax-related recoveries highlights that unpaid tax is and will continue to be an important feature of the Irish model: it prioritizes effectiveness in legal terms, which may mean focusing on cases that are easier to prove rather than those involving more complex or less visible forms of criminality, particularly where there is an extra-jurisdictional dimension.

IMMINENT REFORMS

Given the scale in the growth of financial crime, including the significant increase in push payment fraud, romance fraud, and the use of money mules, as part of a broader multi-agency strategy to tackle financial crime, the Irish Government is legislating to significantly accelerate CAB's asset

forfeiture processes. The Proceeds of Crime and Related Matters Bill 2025 will reduce the deferral period from freezing to forfeiture from 7 years to 2 years, provide for the appointment of receivers when assets are frozen, to prevent respondents from continuing to enjoy the benefit of them, and for the making of payment freezing orders by the District Court. This new regime is expected to come into force during 2026 and should significantly streamline asset forfeiture.

SCALE OF RETURNS

A challenge for the State has been that the contribution of seized assets to the exchequer has tended to be relatively modest, creating a mismatch between the scale of complex fraud and organized crime in Ireland and the level of assets ultimately subject to forfeiture. While no definitive official valuation of the level of financial crime exists, available Garda, CAB, Central Bank and international AML data suggest that the value of financial crime affecting or passing through Ireland in 2026 exceeds €1 billion annually.

And the scale of the problem is growing exponentially, with the number of money laundering reports made annually rising from 50 in 2017 to more than 2,700 in 2025, and 741 money laundering arrests in 2025. Figures for the first quarter of 2026 suggest that these record numbers are likely to be exceeded this year, with active investigations involving gangland figures and their family members and connections, tax defaulters and low-level money mules without previous criminal records.

Despite the innovative structure of the CAB regime, and the fact that the Irish system appears ideally designed to target organized crime and sophisticated fraud, the level of assets forfeited on a per annum basis has been small, for example totaling around €9.8 million in 2023 and increasing to €17 million in 2024, with 2025's figures yet to be released. While such figures must be interpreted with caution—given differences in case duration and the distinction between assets frozen and assets realized, they have nonetheless raised questions about the system's overall efficacy.

A recent advance involving digital assets, however, marks a major step forward for CAB and when taken together with the Proceeds of Crime and Related Matters Bill 2025 may herald a new era of asset forfeiture.

In 2019, gardaí stopped a vehicle in a remote area of County Wicklow, leading them to uncover a massive cannabis grow house operation by Clifton Collins, a beekeeper of otherwise modest means from Crumlin in south Dublin. Following investigations by gardaí into a major energy surge, it emerged that Collins been mining huge amounts of cryptocurrency. In February 2020 CAB successfully obtained orders freezing 12 digital wallets containing 6,000 bitcoin belonging to Collins, then valued at €52m. Collins was jailed and did not resist the Criminal Assets Bureau actions to freeze and seize the Bitcoin. But there was a problem – the encryption key had been lost, having been written on a slip of paper and kept in a fishing rod, which had since been disposed of by the landlord during a clear out of one of the properties. Efforts to retrieve the fishing rod from landfill were unsuccessful. The wallets lay dormant for ten years, with CAB unable to access the underlying Bitcoin.

In a recent breakthrough, however, following a collaboration with Europol in March 2026 the CAB announced that using new technology, it had gained access to one of the digital wallets containing 500 Bitcoin, then valued at €30 million, out of the total holding of 6000 Bitcoin. See Irish Times reporting at. The operation required highly complex technical expertise and decryption capabilities, reflecting the historic difficulty in accessing crypto-assets where encryption keys are unavailable, and benefited from local and international expertise and collaboration. Recent unofficial reports suggest that the authorities may in May 2026 have recovered a further €38.7m from cracking open a second wallet of 500 Bitcoin, the movements of which have been seen on the Blockchain.

These two recoveries dwarf previous annual forfeiture figures, and if CAB's success continues, could see the exchequer receive more than €450m from a single seizure. This represents a major statement of intent by the Irish authorities as to their capabilities and determination to combat financial crime.

This development also demonstrates crime agencies' ability to respond to the evolving concept of unexplained wealth. Crypto-assets have long represented a form of value that can be economically significant but difficult to pin down, combining cross-border mobility with layers of complexity that can frustrate traditional investigative methods. The successful decryption and seizure of this digital wallet places Ireland's CAB at the forefront of international digital asset recovery and demonstrates that, as technical

capabilities improve and cooperation with agencies such as Europol deepens, categories of wealth that were previously resistant to enforcement may become increasingly amenable to forfeiture. The distinction between easy and difficult targets is therefore not static, but contingent on technological capacity and institutional coordination.

THE IMPLICATIONS OF THE NEW EU AML FRAMEWORK

An increased European focus on financial crime should improve the scope for Irish agencies to pursue forfeiture of valuable assets held domestically and across borders. The forthcoming the 2027 EU AML package, comprising the AML Regulation, AMLD6, and the new cross EU regulator (the Anti-Money Laundering Authority, AMLA), which is already operational, should strengthen the practical effectiveness of Ireland's unexplained wealth model by making certain forms of illicit value easier to detect and trace. From July 2027, the new EU Anti-Money Laundering Regulation will apply directly across Member States and extend AML obligations to new categories of obliged entities, including most of the crypto sector and traders in luxury goods, while also imposing an EU-wide €10,000 cap on cash payments. At the same time, the sixth Anti-Money Laundering Directive restructures the national AML architecture and strengthens cooperation between supervisors and financial intelligence units, operating alongside the new AMLA, which has been established to provide EU-level supervision and coordination.

These reforms will reduce some of the evidential obstacles that have historically limited the targeting of concealed or sophisticated wealth. Luxury watches, jewelry, art, high-end vehicles, and crypto-assets can function as stores or transfer mechanisms for illicit value, particularly where cash or opaque payment channels are used. By subjecting more of these sectors to AML obligations and limiting large cash transactions, the new rules will generate more customer due diligence records, more suspicious transaction reports, and better audit trails. For CAB, whose effectiveness depends on identifying wealth disproportionate to lawful income, this may broaden the range of assets that become susceptible to enforcement.

Digital assets pose a particular challenge because while the blockchain is transparent, such assets combine speed, cross-border mobility, and, in

some cases, perceived anonymity. The EU framework does not eliminate those difficulties but brings crypto-asset service providers firmly within the regulated sphere, with associated know-your-customer and due diligence requirement. That may not make crypto-based wealth easy to recover, but should make it easier to detect when illicit proceeds are converted into or out of regulated channels. In this respect, the new EU measures may shift the balance identified in this article: they do not remove the structural preference for assets that are easier to prove, but they may expand the category of assets that are practically capable of proof.

SELECTION EFFECTS AND THE LIMITS OF FORFEITURE

What this analysis shows is that the concept of unexplained wealth highlights a critical limitation of many forfeiture regimes: they do not necessarily target the most harmful forms of criminal activity. Instead, they target the forms of wealth that are most susceptible to legal scrutiny.

This can be understood as a form of selection effect. Enforcement outcomes reflect not only the distribution of criminal activity but also the distribution of evidential accessibility. As a result, forfeiture regimes may disproportionately impact individuals whose financial affairs are more transparent, while leaving more sophisticated actors relatively untouched.

This analysis raises important questions about the purpose, role, and effectiveness of asset forfeiture in Ireland.

On one hand, the focus on evidential practicality is a necessary feature of any legal system. It would be unrealistic to expect enforcement agencies to prioritize cases that are unlikely to succeed in court. From this perspective, the Irish model represents a pragmatic response to the challenges of modern financial crime.

There is, however, a risk that the resulting selection effects may undermine the broader goals of forfeiture. If the system systematically targets easier cases, it may fail to have a meaningful impact on the most serious forms of organized crime, particularly those involving complex financial structures

and cross-border activity. This brings the importance of international cooperation into sharp focus, and the recent collaboration between CAB and Europol demonstrates how transformative such cooperation can be when combined with advancing technical capability. This is important, because when the public sees those widely acknowledged to be actively involved in serious crime enjoying luxury lifestyles beyond their official means, it undermines the rule of law and the authority of the State. In the same way, evidence of valuable assets being successfully forfeited increases public confidence in the system.

CONCLUSION

Asset forfeiture in Ireland is not merely a legal mechanism, but a system inevitably shaped by evidential constraints, institutional design, and the practical realities of enforcement. While it has proven effective in targeting certain forms of unexplained wealth, its operation reflects a broader structural dynamic: what is seized is determined as much by what can be proven as by what is most harmful.

Understanding this dynamic shifts the focus of analysis. Rather than asking whether the system is effective in the abstract, it invites a more nuanced question: effective against what, and under what conditions? The answer lies in the evolving interplay between evidence, technology, and enforcement capacity. As the Bitcoin case illustrates, the boundary between tractable and intractable wealth is not fixed. Rather, it is a function of technological capacity, institutional cooperation, and the willingness to invest in both.

AUTHOR

Karyn Harty is a partner in the Dublin office of Dentons LLP, where she leads the Disputes and Regulatory Investigations Practice Group, and serves as Global Co-Chair of Disputes and Group Money Laundering Reporting Officer for Dentons UK, Ireland and Middle East.

Insider Trading Risks in Big Law: Governance, Accountability, and Enforcement

A Discussion with Professor Karen Woody

ELIZABETH ORTEGA

KAREN WOODY

Introduction

Big Law has not been immune to the insider trading scandals that have engulfed politicians and business executives alike, generating headlines and liability. Prompted by Professor Woody's recent Bloomberg Law analysis examining insider trading risks within major law firms, this Q&A considers how evolving enforcement trends may reshape compliance expectations across the legal industry.

As regulators expand their focus beyond traditional trading activity and toward more complex informational advantages, firms are increasingly confronting questions about governance, surveillance, attorney trading policies, and institutional accountability. The discussion below explores the broader market, legal, and ethical implications of these developments and what they may signal for the future of law firm risk management.

Q: IN LIGHT OF GROWING SCRUTINY AROUND INSIDER TRADING ENFORCEMENT, SHOULD MAJOR LAW FIRMS ADOPT MORE FORMALIZED TRADING COMPLIANCE MECHANISMS—SIMILAR TO RULE 10B5-1 PLANS—TO GOVERN ATTORNEY SECURITIES ACTIVITY INVOLVING ACCESS TO MATERIAL NONPUBLIC INFORMATION?

Prof. Woody: The answer is not an obvious "yes," but the question deserves serious consideration. The recent Big Law insider trading scandal has moved that question from a theoretical realm to a realistic one.

For background, Rule 10b5-1 plans were designed to provide corporate insiders with a structured, affirmative defense against insider trading liability. The idea is that the insider's trades are pre-scheduled, and, as a result, it is presumed that the trader is not trading solely based on material nonpublic information (MNPI). The underlying logic of 10b5-1 plans can be mapped on to law firms, who are arguably in an equally precarious position as that of corporate insiders. For example, an M&A associate routinely possesses MNPI across multiple clients, industries, and deal timelines simultaneously.

A pre-set trading plan, like that of the 10b5-1 plan, would give attorneys a clear, defensible pathway to participate in securities markets without constantly navigating gray areas surrounding insider trading. When a lawyer makes a trading decision months after working on a deal, with only partial recollection of what information she possessed and when, the legal analysis becomes genuinely murky. A pre-established plan eliminates much of that ambiguity.

That said, the 10b5-1 plan is not a perfect fit. Law firms are not corporations, and their attorneys are not trading primarily in their own employer's stock; rather, they are trading across a broad, evolving universe of securities. Designing plans that are both meaningful and workable could pose a significant challenge. The shadow trading problem compounds this: if liability can attach based on economically linked companies, the set of implicated securities expands dramatically, potentially making any compliance plan either unworkably complex or so restrictive as to effectively bar attorneys from market participation altogether.

The takeaway is not that firms must adopt 10b5-1 plans specifically, but that firms should adopt something like a formalized, *ex ante* compliance architecture that takes seriously the scope of their informational exposure. Whether that takes the form of pre-scheduled trading plans, robust preclearance systems, or tiered restricted lists keyed to matter involvement, the key recommendation is the same: compliance must be designed, not assumed.

Q: AS REGULATORS INCREASINGLY FOCUS ON 'SHADOW TRADING' AND INFORMATIONAL ADVANTAGES TIED TO ECONOMICALLY CONNECTED COMPANIES, HOW SHOULD FIRMS RETHINK THE SCOPE OF RESTRICTED TRADING LISTS AND INTERNAL MONITORING PROTOCOLS?

Prof. Woody: The SEC's embrace of shadow trading—the theory that trading in one company's securities can be unlawful because the MNPI one learns in relation to Company A also can apply to Company B because Company B is "economically linked" to Company A -- fundamentally changes the compliance calculus for law firms.

Under a traditional compliance regime, a firm working on an acquisition between two companies would place both companies on a restricted trading list. That list is bounded and manageable. Under a shadow trading theory, the relevant universe expands dramatically: competitors, suppliers, customers, joint venture partners, and potentially firms operating in adjacent sectors may all become implicated. The compliance problem, as I have argued, becomes simultaneously overbroad and underdetermined—overbroad because in theory everything is off-limits, and underdetermined because no one can say with confidence where the boundaries lie.

Firms can respond to this reality in a number of ways. First, restricted trading lists should be rethought to incorporate economic linkage analysis between clients and their competitors and peer companies. This likely requires moving away from static lists toward dynamic, matter-specific assessments. When a deal is opened, the compliance function should engage in a structured analysis of which peer and adjacent companies may be implicated under a shadow trading theory, and the resulting restrictions should be communicated clearly to all attorneys with matter access. Additional monitoring of attorneys' trades, particularly in industries in which the firm has clients, must also be considered.

The deeper implication is that shadow trading forces firms to treat their entire client base as a potential source of compliance liability, and not just the clients with active matters. That is a significant operational shift, and one that requires both technological investment and likely a cultural change within the compliance function.

Q: TO WHAT EXTENT SHOULD LAW FIRMS BE EXPECTED TO IMPLEMENT PROACTIVE SURVEILLANCE TOOLS, TRADING PRECLEARANCE SYSTEMS, OR AI-DRIVEN COMPLIANCE TECHNOLOGIES TO DETECT SUSPICIOUS TRADING ACTIVITY BEFORE REGULATORS INTERVENE?

Prof. Woody: Firms that routinely handle MNPI of the highest commercial value—merger negotiations, securities offerings, litigation strategy—bear a particular responsibility to prevent misuse of that information. The recent scandal involving Big Law attorneys underscored that reliance on attorney

professionalism and ethics standards alone is insufficient. Proactive surveillance is not just good practice; it is increasingly a baseline expectation that regulators, clients, and courts are likely to impose.

Major financial institutions have long operated under compliance frameworks that include personal trading preclearance, restricted lists, certifications, and automated surveillance—all while navigating serious privilege and confidentiality constraints. Thus, the technology exists; the question is whether law firms will invest in it, and whether attorneys will agree to the norm-shifting that will require much more personal disclosure and transparency surrounding their trades.

AI-driven compliance tools could provide streamlined solutions. Machine learning systems can flag trading patterns that correlate with matter timelines, identify anomalous activity by attorneys with matter access, and generate alerts for human review—without requiring direct inspection of privileged communications. Although AI-based systems may still create issues, particularly related to privacy, they represent a meaningful advance over the current norm of manual monitoring and self-reporting.

Ultimately, the standard firms should hold themselves to is proportionality: compliance investment should reflect the firm's exposure to MNPI. Large M&A and capital markets practices create asymmetric informational risk and should be subject to correspondingly robust controls. The days of treating trading compliance as an afterthought are over.

Q: DOES THE EXPANDING INTERPRETATION OF INSIDER TRADING LAW CREATE AN ENVIRONMENT WHERE LEGAL AND FINANCIAL PROFESSIONALS ARE OPERATING WITHOUT SUFFICIENTLY CLEAR BOUNDARIES REGARDING PERMISSIBLE MARKET ACTIVITY?

Prof. Woody: There is a genuine doctrinal instability at the heart of contemporary insider trading law, and it creates real uncertainty for practitioners—including lawyers who are themselves experts in the field.
The core prohibition under Rule 10b-5 has never been defined by statute; it has been built case-by-case through SEC enforcement actions and judicial

decisions. The boundaries of material information, the scope of the duty that triggers liability, and the definition of who qualifies as a "tipper" or "tippee" have all shifted over time, and have varied based on circumstance. Shadow trading pushes the envelope further: it extends liability beyond the securities of the company to which the information directly relates, based on economic linkage theories that are not yet fully settled in the case law.

The result is a legal landscape that is, by any objective measure, unstable. Professionals operating in this environment must navigate uncertainty about where precisely liability begins and ends. For attorneys who deal in MNPI daily, that uncertainty is professionally significant: they cannot always know in advance whether a contemplated trade—even in a company with only indirect links to a current client—will be deemed unlawful based on enforcement theories that may evolve.

Some may suggest that this lack of clarity in the law encourages bad actors. I am not convinced by the argument that unclear law counsels against enforcement. The stronger point is that this doctrinal instability increases the importance of *ex ante* structural protections. If professionals cannot reliably assess the boundaries of permissible trading on a case-by-case basis, the rational response is to build compliance structures that reduce the need for that case-by-case analysis—precisely the logic behind 10b5-1-style plans.

There is also a legitimate policy concern here for legislators and regulators. Continued reliance on judge-made law and aggressive enforcement theories, without clearer statutory guidance, places the burden of navigating uncertainty disproportionately on compliant actors, while sophisticated bad actors continue to find workarounds.

Q: AS FIRMS STRENGTHEN COMPLIANCE OVERSIGHT IN RESPONSE TO ENFORCEMENT PRESSURE, HOW SHOULD THE INDUSTRY BALANCE THE NEED FOR MARKET INTEGRITY AND CLIENT PROTECTION AGAINST CONCERNS SURROUNDING EMPLOYEE PRIVACY AND PROFESSIONAL AUTONOMY?

Prof. Woody: The tension between robust compliance and individual autonomy is real, but it is neither new nor irresolvable. The financial industry has navigated this tension for decades, and the resulting frameworks offer useful precedent.

Personal trading preclearance systems, which are standard practice at major financial institutions, are therefore the most logical first step for large law firms. They require attorneys to disclose proposed trades involving securities that may be implicated by active matters, and they allow the compliance function to identify conflicts before they become violations. When properly designed, preclearance systems generate only the minimum disclosure necessary for compliance review. They likely would not require wholesale surveillance of attorney communications or personal financial accounts.

In my opinion, the professional autonomy concern is somewhat overstated. Attorneys routinely accept constraints on their conduct as conditions of professional practice—conflict checks, confidentiality obligations, competency standards. In order to sit for the bar exam, an attorney must take an ethics exam and often undergo a "character and fitness" review. Trading restrictions tied to matter-specific MNPI exposure are conceptually no different. The question is not whether restrictions are appropriate, but what form they should take and how they should be administered.

Most importantly, the attorney-client relationship creates a fiduciary obligation that encompasses the protection of client information. Strengthening compliance frameworks is not merely a response to enforcement pressure, nor is it a reflection of overzealous micromanagement; it is an expression of that core fiduciary obligation required by all attorneys. Firms that frame compliance investment as a matter of client duty—rather than regulatory risk management—are more likely to build cultures in which the underlying norms are genuinely internalized, rather than merely performed.

PROFILE

Fellow Karen Woody is a professor at Washington & Lee University School of Law. Prior to teaching, she practiced law as a white collar defense litigator in Washington, D.C.

The International Academy of Financial Crime Litigators Founders

For further information, please consult our website:
www.financialcrimelitigators.org

STÉPHANE BONIFASSI
Bonifassi Avocats

LINCOLN CAYLOR
Bennett Jones

ELIZABETH ORTEGA
ECO Strategic Communications