Deloitte.

Combating Illicit Finance
Driving effective response across the judicial ecosystem

Justice Reimagined Series

Contents

Introduction

Illicit finance is money that is illegally earned, transferred, or used to enable crime. The scale of illicit finance is vast. It is the lifeblood of organized criminal gangs whose activities often ruin the lives and livelihoods of millions of vulnerable victims. Illicit finance is a cross border and cross sector problem and impacts all parts of the global economy. Combating a problem of such complexity requires a multisector, cross-industry response. Key stakeholders, including governments and financial institutions, have taken action, but more should be done to drive a more coherent and effective response, including increasing information and intelligence sharing, driving up asset recovery, ensuring public sector investment is commensurate with the threat, and ensuring ecosystem stakeholders have the capacity and skills needed to build an effective framework to tackle illicit finance.

Illicit finance: an overview

The threat posed by illicit finance is not new, nor limited to state actors. Indeed, illicit finance is what enables criminals to profit from heinous crimes and to finance terrorism. It can cause immense financial and human harm to individuals, communities, taxpayers, governments, and the wider society. It is often the most vulnerable, for example those living in poverty or in jurisdictions blighted by corruption, at greatest risk.

The scope of illicit finance is broad. It includes, among others, corruption, money laundering, terrorist financing and fraud, and the statistics paint a frightening picture. Globally, the United Nations Office for Drugs and Crime has estimated the amount of money laundered annually at 2% to 5% of global GDP, putting the total at US$1.9 to US$4.9 trillion.[1] What's more, the landscape is evolving at pace with the rise of increasingly sophisticated cross-border criminality as demonstrated by the widespread abuse of COVID-19 relief by crime groups around the world.[2] The seriousness of the threat is underscored by both its scale (for example, in the UK, fraud is now the number one crime type by volume, accounting for 41% of all recorded crime) and its impact on wider national interests.[3] In the UK, fraud has been reclassified as a national security threat, and is potentially creating over £290 billion in economic damage to the UK economy each year.

Governments are not blind to the threat. Huge sums—US$1.28 trillion of annual global turnover–are being spent by governments to combat the threat of illicit finance.[4] Nonetheless, on average less than 1% of criminal proceeds are recovered annually.[5] The collective failure to deliver effective outcomes against activities involving illicit finance have led some to question whether global responses represent "the world's least effective policy experiment".[6]

A complex problem

Criminal networks commonly operate with speed, identifying emerging vulnerabilities and exploiting them through a mixture of new techniques and technology. In addition, a wide variety of other challenges further complicate efforts to combat illicit financial activity.

1. **A lack of systemwide leadership:** The ecosystem to tackle illicit finance contains a huge number of actors across the public and private sectors with an array of different missions. But a lack of systemwide leadership among justice stakeholders, such as policymakers, regulators, and law enforcement, makes it difficult for those combatting illicit finance activity to coordinate and drive coherent prevention and disruption activity across the whole ecosystem. In addition, real or perceived conflicts between elements of the legal framework (e.g., between the data privacy legislation which broadly seeks to limit the amount of personal information shared, and anti-money laundering rules which can require significant volumes of personal data to be shared) create further tensions.
2. **Information sharing:** In tackling illicit finance, the ecosystem stakeholders are blessed with a data-rich environment: the cleansing of proceeds from a crime (colloquially known as "dirty money") leaves a data footprint, in banks and payment systems. However, much of this data is never shared or aggregated across the justice ecosystem. In addition, key elements of the system (such as globally implemented Suspicious Activity / Transaction Reporting regimes) require those with the least access to threat intelligence to identify risk and "push" reports into government, rather than enabling those with best insight to "pull" it. Information sharing collaborations can help address this issue—but most are in nascent form, and as a result, opportunities to gather comprehensive information and intelligence to disrupt criminal networks are often missed.
3. **The pace of criminal activity:** Many organized criminal groups are experts at exploiting new opportunities with great speed, and are innovating and exploiting new ways to commit crime, using methods ranging from online gaming to romance fraud. Furthermore, as banks have strengthened their defenses in tackling unauthorized fraud (e.g., when a victim's bank card has been stolen) there has been a shift to authorized fraud, for instance where the fraudster persuades the victim to authorize a payment themselves. Illicit financial flows cross borders in seconds, while tracing that money can take years, if it can be done at all, creating a significant disparity between the capabilities of criminals and law enforcement.
4. **A public-private capability imbalance:** The private sector, particularly banks, often have financial crime teams that are well-resourced. Indeed, some banks have financial crime teams that outnumber entire government agencies dedicated to fighting financial crime. But their high-capacity teams require greater access to insights and intelligence if they are to be effectively deployed – they need to know where to look, often requiring the insights and resources of the justice system. In addition, skills in cyber security, forensic accountancy, and financial investigation are in high demand in the private sector, with a significant leaching of critical skills from the public sector.
5. **Regulation:** Financial crime regulation and supervision may have had the unintended consequence of directing system capacity towards the completion of 'tick box' compliance activities that do not lead clearly to the effective delivery of outcomes and interventions against criminals. The flexibility to enable institutions to dial efforts up and down to reflect a changing intelligence picture and national priorities as part of an increasingly intelligence-led and outcome-focused regime is critical.

Current solutions

While these system challenges are considerable, there is growing consensus among policymakers, regulators, law enforcement and the private sector that systemwide reform is essential. There is a growing shift in sentiment and momentum for change around the globe, driven by new legislation, policy changes and public/private sector partnerships. Although the challenges are considerable, policy makers, regulators, law enforcement, and the private sector recently have made some progress in developing solutions.

One such area involves efforts to create systemwide coordination and leadership across all stakeholders in the ecosystem, from regulators to the private sector and citizens. This involves working in collaboration as part of a whole-system approach to drive activities that deliver effective outcomes against clear and commonly agreed upon priorities. For example, consider the UK's Economic Crime Plan[7] and associated governance. Through public private collaboration, system leaders have diagnosed key challenges affecting the effectiveness of the UK's response to illicit finance and agreed on clear recommendations for change including, for example, an increased focus on information sharing, legal reform to drive private sector collaboration, and sweeping reforms to beneficial ownership, which taken together, should meaningfully improve the effectiveness of the entire system.

The information and intelligence silos that exist between ecosystem stakeholders can have a particularly pernicious result: criminals can—and do—exploit them. To help tackle the problem, over the past eight years, a growing number of organizations have proactively engaged in information sharing public-private partnerships (PPPs), creating trusted forums that help to ensure that stakeholders have the information they need to make a difference. And some of these PPPs are scaling and digitizing to increase their impact. Perhaps most significant has been the introduction of information-sharing utilities, such as the Netherlands' Transaction Monitoring Netherlands (TMNL) network. Formed in July 2020 by five Dutch banks, it brings together transaction data to identify unusual patterns of cross-bank activity related to money laundering. Results have been positive. Recently the Bank of International Settlements' (BIS) Project Aurora also demonstrated how leading-edge collaborative analytics could be used to combat money laundering across institutions and borders.

Such utility models are becoming widely recognized as playing a key role in efforts to trace, in real time, information about fast-moving criminal flows of money, creating more opportunities to intervene and recover them. They work because they enable datasets to be combined for collective analysis, enhancing stakeholders' collective ability to identify bad actors and criminal networks. Another good example is the Collaborative Sharing of Money Laundering/Terrorism Financing Information and Cases (COSMIC) digital platform, whose development has been led by the Monetary Authority of Singapore (MAS).[8] MAS has also led the development of a clear regulatory framework to underpin COSMIC, which aims to give confidence to financial institutions in sharing information on high-risk customers and transactions at particular thresholds and aims to help increase disruptions of illicit networks.

Governments have taken significant steps to tackle other important problems as well. For example, the UK's recent Economic Crime and Corporate Transparency Act[9] aims to address the lack of transparent beneficial ownership data that enables illicit activity. The legislation is intended to help prevent the abuse of limited partnerships but also to provide additional powers to seize and recover suspected criminal crypto assets, improve the effectiveness of Unexplained Wealth Orders (a non-conviction-based asset recovery mechanism), and enable new intelligence-sharing powers for law enforcement and the private sector. And in the US, to help focus finite resources on more serious financial crimes and deliver a more sustainable model in terms of time, cost, and outcomes, the Anti-Money Laundering Act of 2020 has introduced the concept of national anti-money laundering (AML) and combating the financing of terrorism (CFT) priorities. Once refined, these priorities can help the regulated sector focus its capacity where law enforcement most needs it. A similar innovation is also set out as a key action in the UK's latest Economic Crime Plan 2 (2023-2026).[10]

Recommendations

The global response to illicit finance is at an inflection point. The scale and impact of illicit finance activity is growing, and the poor outcomes being achieved against the threats resulting from it are such that more can be done. A whole system approach is needed with all ecosystem stakeholders (regulators, supervisors, law enforcement, policy makers) enabled to maximize the impact they can have on delivering outcomes against criminals. Recommendations for change include:

Prioritizing clear system leadership. That means having a system leader that can bring together the whole ecosystem to create a cross-industry response to a cross-industry problem, with collaboration to drive forward toward an agreed ambition.

The role of the system leader is to identify and bring together the policymakers, enforcement agencies, regulators and private sector. The task then is twofold: 1) to facilitate the alignment of stakeholders around a set of priority threats and activities; and 2) to help ensure that the participants collaborate effectively. This means that organizations contribute to the cause (which could include intelligence, resources, funding) and also benefit from their involvement (which could include clearer guidance from supervisors, or a smaller volume of better-quality intelligence referrals).

The approach in the UK has been to bring leaders of key organizations together in a workshop setting, to build a shared view, establish trust and codify ways of working. This is helping to embed this shared endeavor in joint governance and start to shift the collective approach to one of cooperation for mutual benefit.

Improving information-sharing. PPPs still operate in quasi-pilot form: small scale, voluntary, analog and delivered in addition to day-to-day wider financial crime obligations. To reap the benefits of their collaborations, they should be recognized and incentivized by policymakers and regulators as a key component of a healthy financial crime framework. To help with this, the Financial Action Task Force (FATF), the global money laundering and terrorist financing watchdog, should formalize the role of PPPs within the global framework to encourage senior political engagement and funding for their development, and to help ensure wider engagement from key stakeholders in the national AML ecosystem. Over time, public private engagement should become a fundamental component of the whole system response, with collaboration embedded in policy and legislation as well as in the development of both strategic and tactical intelligence capabilities. To accelerate this process, it is critical also that stakeholders are incentivized by the regulatory framework to engage in these high-value activities, establishing them as an integral part of an effective financial crime framework.

Accelerating progress also requires more work to be done to resolve tensions between data protection and AML legislative frameworks—allowing parties to exercise a right to privacy, while also helping ensure they can access a right to be protected from crime. Finding safe ways to enable more information and intelligence to be shared between system stakeholders is critical to improving outcomes.

Enabling faster action. Information sharing utilities are mechanisms that either allow duplicative processes to be undertaken once on behalf of many (e.g., Know Your Customer (KYC) utilities), or which allow otherwise siloed datasets to be brought together (both public-to-private and private-to-private), either through data pooling, or through the use of collaborative analytics, to enhance the efficiency and effectiveness of risk management functions. While the creation of completely new, custom built information sharing utilities offers significant long-term potential, a faster outcome could result from leveraging existing points of data aggregation in the financial system, where data from across multiple institutions already resides in one system. Avoiding or reducing the upfront challenge of first needing to bring data together could result in more quickly realizing information-sharing benefits. The payments architecture could offer such an opportunity, which justifies exploring this option further.

Incentivizing and enabling the investment in technology may also be critical to unlocking the potential of big data, to leverage the use of advances such as AI and machine learning to interrogate data for pattern recognition and network identification.

Enhancing transparency of beneficial ownership. Greater progress should be made to help ensure national beneficial ownership registers, in jurisdictions where they exist, as seen as are trusted sources of accurate and reliable data, which can be accessed globally to understand ownership structures. Register owners could build their own 'know your customer' capabilities to support effective registration, with two-way sharing, and resolution, of data discrepancies with private sector data holders (e.g., if a bank's record of beneficial ownership materially differs from that held by the central register). Thus an accurate beneficial ownership register, in jurisdictions where they exist, is a critical piece of infrastructure to support the fight against illicit finance activity, helping support prevention activity—from sanctions evasion to fraud.

Improving rates of asset recovery. Recovering assets requires bringing investigators with high-end skills to the table—forensic accounting, asset tracing, cyber, and an ability to access and analyse open-source intelligence. But they tend to be in short supply in the public sector. For that reason, more investment in public sector capacity is key. Also important is exploring better ways for the private and public sectors to collaborate to track, trace, and recover more assets. Innovative concepts, such as the development of shared workforce strategies across the illicit finance ecosystem, are in their infancy but have great potential and should be further explored.

Boosting public sector funding. Illicit finance activity is commonly described as a national security issue but is not commonly funded accordingly. An increase in funding could be partially recuperated by reinvesting money gained from improved asset recovery. Stakeholders should also think about implementing more innovative ways of funding improvements in the system such as, for example, appropriating funds in suspended accounts and using them for law enforcement. Another example would include the Economic Crime Levy[11] that has been introduced by the UK Treasury with the aim of raising £100 million per year from the AML-regulated sector to help fund government initiatives set out in the Economic Crime Plan to tackle financial crime. While an effort such as this can be challenging to implement, it might provide a revenue stream to uplift capabilities.

The world of illicit finance is a complex, multifaceted ecosystem with a web of fast-moving actors. For that reason, combatting the problem is a massive undertaking, requiring a coordinated, multisector, global response. But sufficient cooperation among public and private-sector entities to build on existing efforts is a big step toward success in this area.

Contacts

Beth McGrath
Global Government &
Public Services Leader
Deloitte Global
bmcgrath@deloitte.com

Andrew Colvin
Partner in Financial Advisory
Deloitte Australia
ancolvin@deloitte.com.au

Chris Bostock
Director
Deloitte LLP
cbostock@deloitte.co.uk

Rebecca Green
Director
Deloitte LLP
rebegreen@deloitte.co.uk

Tim Newman
Director
Deloitte LLP
tnewman@deloitte.co.uk

Endnotes

1. Europol, "Money Laundering," 2022.
2. Interpol, "Unmasked: International COVID-19 fraud exposed," April 2020.
3. House of Lords Committee Report, "Breaking the Fraud Chain," November 2022.
4. Refinitiv (May 2018) 'Revealing the True Cost of Financial Crime: 2018 Survey report, p. 26
5. Interpol, "International crackdown on West-African financial crime rings," October 2022.
6. PoI, "Anti-money laundering: The world's least effective policy experiment? Together, we can fix it.".
7. Gov.uk, "Economic Crime Plan 2 2023-26," March 2023.
8. Monetary Authority of Singapore, "COSMIC," December 2023.
9. Legislation.gov.uk, "Economic Crime and Corporate Transparency Act 2023," October 2023.
10. Gov.uk, "Economic Crime Plan 2 2023-26.".
11. Gov.uk, "Get ready for the Economic Crime Levy," July 2023.

Deloitte.