ORGANISED AGAINST CRIME

COMBATING ILLICIT FINANCE

THE IRISH PERSPECTIVE ON

ILLICIT FINANCE

All industry players must collaborate better to be effective in the fight against illicit finance.

DEIRDRE CARWOOD
PARTNER
FINANCIAL ADVISORY
Deloitte Ireland

LAURA WADDING
PARTNER
RISK ADVISORY
Deloitte Ireland

As criminals become increasingly sophisticated, they're finding new ways to channel illicit money through legitimate banks. In the process, they're managing to stay one step ahead of the industry. This has a potentially significant impact on Ireland, given its role as a dynamic international financial services hub: a leading player for wholesale banks and investment funds and part of a heavily intermediated international financial landscape.

Over the past two decades, financial institutions based in Ireland have spent a lot of time raising their standards to comply with increasing anti-money laundering (AML) regulations, keeping customer documentation up to date, and remediating issues as they arise. Every year, financial institutions invest a large proportion of their costs into maintaining this

Simply complying with regulations doesn't prevent a bank from becoming a victim of crime.

regulatory compliance – but simply complying with regulations doesn't prevent a bank from becoming a victim of crime. And the fight against financial crime has become fully digital, following the changed working models after COVID-19 leading to an accelerated shift towards fully digital environments.

But have the banks' systems kept pace? Are their internal control frameworks strong enough to track suspicious data points, and highlight transactions that seem out of the ordinary? In the physical world, a human employee could compare a passport photo with the person standing in front of them waiting to make a deposit. Face to face contact and human interaction have been very effective in identifying suspicious activity in the past. In the digital world, we rely on algorithms to spot that activity and mark it as unusual. For example, if an account that has had regular monthly lodgements of €10,000 suddenly has deposits of €150,000 at a time, that's a potential red flag. This kind of detection technology can be costly, and large financial institutions can be slow to adapt.

Another way for financial institutions to detect potential illicit financial flows and identify emerging trends in criminal activity is through information sharing. However, the data sharing forums currently in place are not fit for purpose and they need to be much broader in scope for today's digital world.

Retail banks, FinTechs, regulators, accountancy practices, legal firms and law enforcement all have their own discussion forums but there is no single, central utility gathering information, detecting patterns and developing typologies of illicit finance activity.

This matters, firstly because without a unified forum, the lack of up-to-date near-real-time sharing of information between all stakeholders is causing delays in investigating suspicious sources of money.

Secondly, it also makes it difficult to measure the cost of financial crime, and specifically illicit finance, to the industry and the economy. In an Irish context, when the Garda National Economic Crime Bureau reports instances of financial crime to the Central Statistics Office, this tends to appear as one number, so we don't have a breakdown of illicit finance. Similarly, financial institutions may be obliged to report issues around illicit finance to the Central Bank of Ireland, but there is no aggregate data that is shared in the appropriate circles.

But if data can be a help in the fight against financial crime, it can also be a potential hindrance. Under the General Data Protection Regulation, organisations are only entitled to collect the information they need to retain based on the business requirements. The more personal information a bank holds about its customers, the greater their obligations are from a data protection perspective.

This is a difficult balancing act: how far should a bank go to demonstrate that it knows who its customers are? The delicate line between properly addressing the threat of illicit finance and respecting the individual's right to data privacy is set to remain a key issue.

Read on to learn more about combating illicit finance from a global perspective.

WHY ORGANISED ILLICIT FINANCE DEMANDS AN ORGANISED GLOBAL RESPONSE

CONTRIBUTORS

BETH MCGRATH
GLOBAL SECTOR LEADER FOR THE DEFENSE, SECURITY & JUSTICE SECTOR
United States

ROBERT CONTRI
GLOBAL FINANCIAL SERVICES LEADER
United States

CHRIS BOSTOCK
DIRECTOR, GOVERNMENT & PUBLIC SERVICES
UK

TIM NEWMAN
DIRECTOR, GOVERNMENT & PUBLIC SERVICES
UK

A system is only as good as its weakest link. Which is why it's vital that all system stakeholders collectively – and quickly – address their current weak spots.

Illicit finance is a major threat to the security and prosperity of all nations. It not only enables criminals to profit from the most heinous crimes, but also finances terrorist atrocities. It causes an immense financial and human cost to society, business and government; a cost that we cannot, and should not, bear.

Organised financial crime prevails over a disorganised system

In an increasingly interconnected, digital world, those engaged in financial crimes are continuously evolving their international operations, working across multiple jurisdictions. They act with a speed and sophistication with which the siloed 'system' – government, law enforcement, regulators, corporates, and financial institutions – struggle to keep pace. For example, the Financial Action Task Force (FATF) has identified just how quickly criminals have exploited the COVID-19 pandemic to commit fraud and money laundering.

Despite some excellent examples of successful collaboration, strategic system-wide cooperation continues to be needed. Less than 1% of the billions of dollars laundered annually are ever recovered (Source: Global Initiative Against Transnational Organized Crime).

The regulated sectors, for instance, financial services, have taken significant steps to protect customers and the economies in which they operate. Investment in people, processes, and technology to monitor customer transactions for signs of risk has been huge, and regulatory pressure has been high. Despite this, it has proven extremely difficult to effectively stem the flow of illicit finance.

The word 'flow' here is appropriate. Like water, financial crime always takes the path of least resistance, quickly finding its way into the cracks. And a system is only as good as its weakest link. Which is why it's vital that all system stakeholders collectively – and quickly – address their current weak spots.

Crucially, this requires a commitment from all parties to take an empowered, proactive stance rather than a defensive, reactive one: to own a common ambition and approach, effectively sharing intelligence on individuals and groups so financial crime can be tackled swiftly. Strong international leadership is vital, and it is encouraging to see the fight against illicit finance in all its forms as an area of focus for the new administration in the US.

Only by working collectively as a single, coordinated system can public and private organisations effectively fight illicit finance. Only together can we change how it's perceived, opposed, and prevented.

This article was first published by Forbes '[Why Organized Illicit Finance Demands An Organized Global Response]', May 2021.

Five steps to collectively tackle illicit finance

From Deloitte's engagement across the illicit finance regime, we believe there are five key steps which the ecosystem should take collectively in response to the threat.

1. Improve alignment

A greater alignment of preventative effort across the public and private sector, concentrating on high-value activities, is paramount.

This should include better sharing of information and intelligence, such as emerging typologies and tactical data sets, which would sharpen the regulated sector's ability to identify suspicious activity.

Anecdotally, some banks report that as little as 1% of transaction-monitoring alerts identify information that warrants reporting to national intelligence authorities, suggesting significant effort and capacity in the system is arrayed against activity that does not lead to outcomes.

2. Renew the focus on effectiveness

In some cases, the ability to align resource to where it's needed most is inhibited by legislative and regulatory frameworks, or their interpretation.

It is important that financial crime risk management frameworks are implemented by organisations and regulated to prioritise the effective delivery of outcomes rather than focusing on technical compliance as an end in itself.

There are encouraging signs that innovative approaches are being considered and progress is being made, such as within the Deloitte US's recent consultation on enhancing the effectiveness of Anti-Money Laundering (AML) programmes.

3. Increase collaboration

The adage "the whole is greater than the sum of its parts" is certainly true of the illicit finance regime.

Improved collaboration could also enable global public sectors to leverage the capacity and capabilities of the private sector to help drive a more disruptive agenda and secure better outcomes. As an example, global law enforcement could look to the approach taken by the US Department of the Treasury and Department of Justice (DoJ). The DoJ has worked with the private sector for the best part of a decade, bringing in forensic accountants, open-source intelligence analysts and more, which has enabled them to make a dramatic step-change in the seizure of criminal assets.

4. Embrace new technologies

While the proliferation of emerging technologies, including new payment platforms, cryptocurrencies and Digital ID, represent criminal opportunity – with Treasury Secretary Janet Yellen commenting that when Bitcoin is used "it's often for illicit finance" – it also provides an opening for the ecosystem to start designing out vulnerabilities.

Emerging analytics and encryption technologies will allow us to "see more" in data and enable new kinds of data sharing in compliance with overarching privacy principles.

5. Make broader connections

Illicit finance requires all sectors to play a strong, active role. This goes beyond financial services, governments and law enforcement. Within the global corporate sector social media, Internet Service Providers, and telecommunication companies can all be vectors through which fraudsters access their victims. All have a preventative role to play.

The challenge is significant and requires considerable reform of the current system. But from Deloitte's experience of working with organisations across the ecosystem, we know that everyone involved wants the same outcome: to prevent crime, protect citizens and customers, and disrupt the criminals. The task, for leaders in both governments and industry, is to harness their shared ambition and go on this transformational journey together.