Commercial feature

Tackling financial crime through collaboration

Taking a joined-up, data-led approach is key to addressing the rising problem of financial crime

Financial crime is a multi-trillion-dollar business for criminal organisations. Annually, the proceeds from their illicit activity laundered through global financial networks are worth between 2-5% of global GDP. As a result of the loss and harm this is causing society, fighting financial crime has become a key priority for many governments, including in the UK.

Just to remain compliant, financial institutions have been investing heavily in their financial crime programmes for the last 20 years. At the same time, the costs of compliance have continued to rise exponentially. Despite all this investment, driven largely by regulatory pressure, it's not enough. The value of illicit funds confiscated or disrupted is still well below acceptable levels and more needs to be done to tackle the problem.

The challenge for firms is to both create a more effective financial crime programme and drive efficiency. What may look like two competing agendas can, however, be delivered using technology and data. With a big focus by regulators and policymakers on technical compliance as well as demonstrating effectiveness in disrupting financial crime, alongside an internal agenda on cost optimisation, the spotlight on digital transformation has never been stronger, says Geraldine Lawlor, global head of financial crime for KPMG.

More mature organisations are currently moving towards data and technology-enabled process transformation. This is where the future appears to be. However, it requires some brave decisions to be made on legacy infrastructure. It also requires a move away from the silo mentality, bringing the organisation together in terms of how it views and manages this risk. For some, this may be a paradigm shift, but for others, it's a necessity.

To support this change, the traditional limitations on data from product-led legacy systems are being overcome by tools that leverage and enrich existing data sets. This allows the data to be used more effectively. "Banks are also moving from traditional approaches to monitoring transactions to looking at networks of activity, connecting relationships and observing illicit activity across a network that was not evident at a transactional level," says Ignatius Adjei, UK fraud technology lead at KPMG.

The focus on data is fast becoming a fundamental part of how organisations better manage their financial crime risks. Their know your customer (KYC) programme is at the heart of this. "Rather than see it as an exercise in identification and verification aligned to technical minimums, it should be viewed as the data source to manage all subsequent downstream processes that support better detection, disruption and optimisation," says Lawlor.

Another emerging theme is convergence under an economic crime lens. This covers a collection of risks; namely fraud, money laundering, counter-terrorism, market abuse, sanctions, bribery and corruption and tax evasion. It is a means by which organisations are starting to recognise that managing risks in isolation is not the answer. They need to have a new way of assessing how to deliver greater efficiency.

"We are seeing this convergence, with fraud and cyber-enabled crime moving closer to anti-money laundering, particularly around mules," says Adjei. This is reflected in the mindset shift towards the need for greater collaboration. It's supported by access to enriched data, information and intelligence, and enabled by better tools. As a result, firms' ability to manage risks and threats is improving.

With the focus on innovation and cost optimisation, the role of the compliance function is also evolving. There is an increasing trend towards moving activity out of compliance and into shared services. Doing so enables firms to drive operational standardisation and convergence, leveraging common tools and management structures, and positioning for greater efficiency.

However, this transition can have its challenges, and "it is important to set clear outcomes, good design principles and agreement around how accountability, responsibility and oversight need to work," says Lawlor. "It is, however, worth the effort, as it brings an organisation together and makes the business accountable for client risk. It also allows compliance to move to an oversight role, while driving an optimisation agenda through operations, leveraging data and technology to full effect."

Alongside the work currently being undertaken within organisations, regulators are also playing a key role in supporting and encouraging innovation to better manage the negative effects of financial crime. As organisations start to improve the way they respond to and work with their regulators, these relationships will evolve positively. "When you start to bring them into the conversation, there becomes a real opportunity to drive a much healthier relationship where we are all on the same side. We're part of an eco-system that is working together against the common threat: the criminal," says Lawlor.

To further support collaboration, there has been an emergence of public-private partnerships across a number of jurisdictions, with the UK taking the lead. Reform is also high on the agenda, underpinned by the legal changes coming through under a series of economic crime bills. A key component of such reform will be the ability to share information and intelligence more routinely and to put it to use. There's already a huge amount of work underway here. Without it, the ability to join the dots across the financial marketplace and, ultimately, disrupt criminal networks remains limited.

Success in driving down the negative effects of financial crime comes from the will of all the stakeholders to change and evolve collectively. It's amazing what can be achieved when everyone pulls in the same direction. The loss and harm to society needs to stop, and our economies need to be able to prosper and grow. Moving forward to an environment built on collaboration, enabled by data, intelligence and the right tools, will be critical to achieving this.

2–5%

of global GDP comes from the proceeds of criminal organisations' illicit activity laundered through global financial networks each year

> **The loss and harm to society needs to stop, and our economies must be allowed to prosper and grow**

For more information about financial crime visit home.kpmg/uk/en/fincrime

KPMG

REGULATION

Crypto-crime crackdown increases

Enforcement actions are increasing as global regulators step up their efforts to supervise the crypto market, while some jurisdictions are adopting a more crypto-friendly approach

Ben Edwards

Yuichiro Chino via Getty Images

With the value of the global cryptocurrency market north of $3tn (£1.09tn) and mainstream crypto adoption continuing to accelerate, global regulators are racing to keep up.

In March, President Joe Biden signed an executive order that tasks the entire US government with forming a strategy to regulate digital assets, including cryptocurrencies. Meanwhile, in Europe the EU is in the process of finalising its markets in crypto assets legislation, which seeks to oversee crypto activities that fall outside existing regulations. The UK's FCA also earlier this year proposed tougher rules on crypto advertising, to stamp out false or misleading claims.

"Those who are new to this or just pressed for time will say crypto is unregulated – nothing could be further from the truth," says Marco Santori, chief legal officer at Kraken, a crypto exchange.

Much of the early regulatory agenda for cryptocurrencies and the emergence of blockchain technology focused on money services, though since 2017 with the boom in initial coin offerings, that has started broadening into areas such as capital formation, says Santori.

"There are new, emerging uses of blockchain technology that implicate new risks and are creating new industries – it's those emerging uses that are under regulatory scrutiny," he says.

But given the rapid pace of crypto adoption, regulators have struggled to keep pace. "Regulation has lagged but as Biden's order indicates, there is a growing awareness that there needs to be a much tighter regulatory framework around crypto," says Ben Richmond, founder and CEO of regtech company Cube Global.

Enforcement actions are also starting to increase. The US Securities and Exchange Commission (SEC), for instance, has brought around 100 cryptocurrency enforcement actions since 2013. The agency's new chairman, Gary Gensler, said the SEC hopes to start regulating crypto exchanges this year.

> **New uses of blockchain technology implicate new risks and are creating industries. It's those emerging uses that are under regulatory scrutiny**

"Learnings from those actions are driving regulator behaviour, but that's where it risks becoming fragmented because you can end up with different approaches to the same problem," says Richmond.

Another debate has fizzed around how to regulate crypto. Should it be bolted on to existing regulations or regulated as a separate industry, with its own regulator and laws? Timothy Spangler, a US-based partner at law firm Dechert, believes it should be the former.

"I would rather spend more time understanding the technological impacts than creating new regulators, new crimes and new oversight mechanisms, and then having to debug those over the course of years and years," he says. "That could unnecessarily stymie innovation."

Others argue that the novelty of blockchain technology means it shouldn't be shoe-horned into current regulations.

"Most regulators are using a traditional approach to regulate crypto," says William Je, CEO of Hamilton Investment Management. "But crypto is creating new financial products that are entirely different to anything that has come before."

Some jurisdictions are taking a more active pro-crypto stance to attract crypto businesses, such as US state Wyoming, which has passed a series of crypto-friendly blockchain laws.

"Wyoming has taken a descriptive rather than a prescriptive approach to regulation and is a model for other jurisdictions," says Santori.

One initiative Wyoming has adopted is creating a banking license that tailors the regulatory regime to the actual risks of the bank. For instance, Kraken was the first crypto company to receive a license under the state's new banking charter aimed at digital asset businesses, which allows them to take deposits as opposed to make loans. "It dials up oversight of reserves and forgoes the regulations usually required for banks that lend," says Santori.

A focus on crypto-mining activities, particularly around energy use, is also attracting the attention of regulators. China has banned crypto mining, while the EU considered banning certain energy-intensive methods for mining crypto but has since backed down.

"To say that we need to regulate crypto miners is to say that crypto mining poses a danger, but we're a long way from quantifying that," says Spangler. "How comfortable are we that we accurately know the energy usage that miners engage in? Most of the academic surveys are qualified and speculative."

While regulatory best practice is a work in progress, Spangler believes those jurisdictions that tread cautiously are likely to yield more effective long-term outcomes.

"We need to move at the right pace to make good decisions," he says. "We want to move forward based on knowledge. Move slowly and roll out things as needed – we don't know where blockchain will move."

But while the US has traditionally set the standard for global financial regulation, it is not a given that it will shape how crypto regulation develops worldwide.

"Most people would agree that crypto's centre of gravity initially was the US and Canada. But there's no reason why, having created a new technology or protocol, they would also win the deployment," Spangler comments.

A lack of regulatory harmonisation across jurisdictions is also potentially weighing on the growth of the crypto market."Every country has different rules and regulations – or even definitions – of what should be regulated, so at the moment it's not clear, which is holding back institutional investors from investing in crypto," says Je. "This is the biggest hurdle for the development of crypto, so we need more clarity."

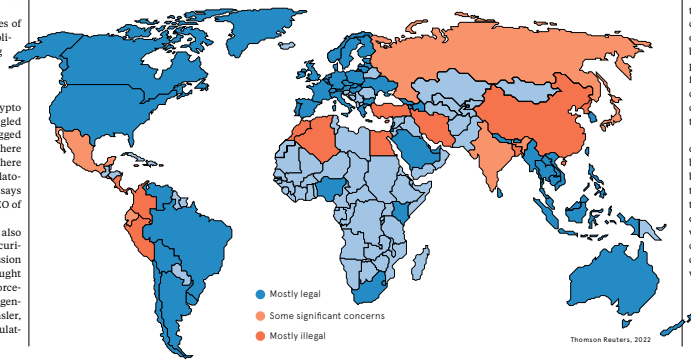
Others believe that while regulation is necessary to safeguard consumers, it could slow the pace of adoption. "It's about getting the balance right. How do you protect people but enable this world to flourish?" says Richmond. "The concern is that if the regulation comes in too hard, it will slow down the uptake."

Worries that too much regulation could choke innovation are likely to be overblown, though Santori believes some innovation will inevitably be constrained as regulators tighten their grip. "That's the trade-off when we regulate," he says. "But we also create a more stable and welcoming environment, so that is the correct lens to view the decision of whether to regulate."

As blockchain technology continues to thrive and new use cases emerge, one thing is certain: the regulatory backdrop is far from resolved.

CRYPTO REGULATION WORLDWIDE

Level of cryptocurrency regulation by country



Thomson Reuters, 2022