Derville Rowland: Innovation and technology in financial crime

Remarks by Ms Derville Rowland, Deputy Governor of the Central Bank of Ireland, at the Afore Annual FinTech and Regulation Conference, Dublin, 4 February 2025.

* * *

Good afternoon, ladies and gentlemen. It is a pleasure to be with you today and to address a topic so crucial to the future of financial services: the utilisation of innovation and technology to conduct – and most importantly, combat – financial crime.

In the mid to late '90s, when email truly took off as a global tool for commerce, I was a barrister working for the UK's Crown Prosecution Service amongst others, dealing with various criminal cases including serious frauds.

Justified enthusiasm about the ability to connect the world more effectively and efficiently was subsequently dampened somewhat by use of the technology for all manner of deceptions, frauds and financial crimes.

Several decades later, we see the same pattern playing out in real-time with artificial intelligence, with criminals using AI tools to bypass customer due diligence controls and carry out fraud via social engineering.

These sophisticated methods, including the use of AI tools via text, images, and voice, present significant challenges for regulators and supervisors.

There's a popular saying that the pessimist complains about the wind, the optimist expects it to change, but the realist adjusts the sails.

As a regulator with hard-won experience of developing frameworks, building the teams to implement them, and deploying technology to combat financial crime and address misconduct, I'm very much a realist – albeit one who remains stubbornly optimistic. I don't believe it's an either/or scenario.

Put simply, I believe in the potential benefits of innovation and technology for consumers, investors, businesses and society – and want to see them realised. But this also means the risks must be effectively managed – we must, as it were, adjust the sails.

The importance of collective responses

The risks, of course, need no explanation to this audience. The anonymity of virtual assets can be used to transfer illicit funds quickly and across borders, with criminals increasingly leveraging new technologies to commit fraud, launder the proceeds of crime, and carry out financing of terrorism. The speed at which funds can be moved across borders makes it easier for criminals to exploit the financial system. And so on.

Last month, the Central Bank of Ireland published statistics showing the value of fraud in payments in Ireland increased by a quarter in 2023 compared to 2022 – from €100m

to circa €126m.[1] Fraud was highest in credit transfers and card payments, with the biggest growth seen in money remittance.

This echoes trends across Europe, with a joint EBA/ECB report in August 2024 revealing that fraud losses are highest in credit transfer and card payments across the European Economic Area (EEA).[2]

Financial crime, of course, recognises no borders. And so, given the scale of the challenge which regulators and law enforcement agencies face, collective action – a harmonised response - is imperative.

Which is why the EU's AML package is so important – it provides the framework and the agency (AMLA) through which we will collectively meet the challenge head on.

The AML package is by design technology neutral. It applies to traditional banking /financial models equally as it applies to crypto-asset service providers (CASPs), crowd-funding platforms and intermediaries. It obliges all types of firms that come within its ambit to comply with a set of AML/CFT rules that have now been harmonised across Europe.

How these firms comply with the rules is up to them, via traditional AML/CFT compliance programmes or by using regtech tools. What's essential is that the means used are effective, and that such effectiveness can be demonstrated to supervisors.

This will be the case both for the 40 obliged entities that will be directly supervised by AMLA and the firms supervised by national AML authorities.[3]

Not waiting for the wind to change, the EU has addressed a number of emerging risks in the package.

To give some examples, the use of AI is acknowledged under the package, with an obligation on firms to ensure that human oversight is applied to decisions proposed by AI tools that may impact customers in certain areas.

Additionally, details of Virtual IBANs which are linked to other payment accounts will have to be recorded in member states' Bank Account Registers. This will allow law enforcement to trace any funds being moved by such Virtual IBANs.

Finally, the package introduces the concept of Information Sharing Partnerships. Through these, credit and financial institutions will be enabled to share information relating to high risk customers, subject to important guardrails including data protection assessments.

The lack of an ability to share such information has long been pointed to as a real weak link in the system, which could allow someone who had an account closed by one bank on ML/TF grounds to seek to open an account in another.

It is hoped that these partnerships will be a real game-changer in the fight to keep bad actors from accessing the financial system in order to launder ill-gotten gains. Tech solutions, including tools which can allow information to be shared between financial institutions in a manner that complies with GDPR, will be essential here.

The package is also forward-looking in respect of sanctions.

Russia's illegal war against Ukraine exposed some fault lines in the EU's Financial Sanctions Framework. The package seeks to remedy this by imposing obligations on obliged entities to put in place frameworks to prevent and detect attempted breaches of EU financial sanctions.

It also requires obliged entities to ensure that prospective customers, and any person who owns or controls such prospective customers, are screened against the financial sanctions list prior to onboarding. Here again, we see the importance of effective technological solutions - the use of screening tools will be imperative for firms seeking to protect themselves from the possibility of breaching sanctions.

Developing a wider approach to preventing financial crime

Money laundering pre-supposes a predicate crime which has generated assets for a criminal. Looking more widely across the landscape, more work is required to put in place a comprehensive financial crime preventative framework that includes fraud.

The EU and member states have started thinking about fraud and money laundering more holistically, rather than two silos to be tackled independently. This is very welcome.

For our part, the Central Bank of Ireland is approaching AML, fraud, and sanctions through the lens of financial integrity of the system. We are building out a more integrated supervisory framework to look at risk in a more holistic way. We want to take a whole-of-sector, rather than piecemeal, approach, and so very much support emerging EU thinking in this area.

As a single market and economic and political union, the EU can point to work already under way and leverage further opportunities to confront the challenges involved.

Already, there are a number of other important EU developments aimed at protecting the financial integrity of the system and the citizens who depend on it.

PSD3 and the Payment Services Regulation will strengthen customer authentication rules and extending refund rights of consumers who have fallen victim to fraud, among other measures.

The EU's Markets in Crypto Assets Regulation (MiCAR) includes rules relating to the information to be made available to prospective investors in crypto assets, partly in response to the proliferation of scams involving crypto asset issuance.

The amended Fund Transfer Regulation ensures that transfers of crypto assets by CASPs must now be accompanied by information on the sender and recipient, in the same way that credit transfers between banks must be.

The Instant Payments Regulation (IPR) obliges providers of standard and instant credit transfers to verify the payee at no additional charge to the payer. It also obliges PSPs offering instant credit transfers to screen their customer base against targeted financial sanctions lists at least daily.

The various regulatory and policy developments to tackle financial crime cannot succeed in isolation. For this reason, supervisors have been on a steady march away from reliance on traditional supervisory tools and are increasingly exploring ways to transform technology from an enabler of financial crime to a tool in the detection, disruption and successful prosecution of financial crime.

In that context, I'd like to mention a significant milestone in the Central Bank of Ireland's innovation journey - the launch of our Innovation Sandbox Programme last December on the specific theme of Combatting Financial Crime.

About the sandbox

This initiative offers a structured environment for firms to develop innovative solutions in a collaborative environment, ensuring that new technologies are introduced safely and effectively into the financial sector.

The seven participants in the programme are employing new technologies and innovative methods to develop solutions that tackle financial crime, for the benefit of both the financial system and consumers.

Participants are representative of a diverse spectrum of innovators from Ireland, across Europe and the UK and feature start-ups, scaling firms, partnerships and established financial services firms.

Although it is still at an early stage in the programme, several key areas of focus have been identified such as:

- The use of AI, machine learning, and pattern recognition to detect and prevent fraud; and
- The use of technology to enable data sharing without compromising sensitive information, allowing real-time verification of identities and other credentials while ensuring full compliance with data protection regulations and the development of digital identity verification tools.

The Central Bank is organising workshops for participating firms on specific topics relevant to theme of combating financial crime, facilitating bespoke engagement with dedicated relationship managers, and providing access to a data platform offering data sets and tools relevant to the theme. This will allow participants to test and develop their innovation.

We are hugely excited about the programme and look forward to sharing the results of it in due course.

Conclusion

In conclusion, I was greatly struck by something Elizabeth McCaul of the ECB Supervisory Board previously said: "Technology is fundamentally a human activity-technology is neither good nor bad, but humans make it so." [4]

The reality is that no piece of legislation can contemplate every financial crime risk or typology or close every loophole. We can't wipe out financial crime – any more than we can wipe out car theft, shoplifting or burglary. But what we can do is to become as effective as possible at reducing its impact.

Hence, as technology evolves, it behoves regulators and supervisors to evolve too - continually adapting to keep pace with these changes and ensure that, collectively and individually, we are the forefront of protecting the integrity of the financial system and those who use it.

Thank you.

---

[1] Behind the Data – Insights from Irish Payment Fraud Statistics

[2] EBA and ECB 2024 Report on Payment Fraud

[3] The 40 obliged entities will comprise the highest risk entities operating across the EU and at least one entity from each Member State.

[4] ECB Supervisory board - Technology is neither good nor bad, but humans make it so