Fighting Financial Crime: Why Technology — and AI — Give Us Our Best Chance

Author: Rachel Woolley, Chair of Compliance Institute's Financial Crime Compliance Working Group.

Financial crime isn't just evolving – it's accelerating. Its scale, complexity, and global reach now far exceed the capabilities of traditional controls. Organised criminal networks are exploiting fast-moving digital economies, new payment technologies, and regulatory gaps, moving illicit funds at a speed and agility that outpaces traditional controls.

For compliance professionals, this creates a difficult reality: the methods that worked a decade ago no longer offer meaningful protection today. Static rules-based systems, manual reviews, and after-the-fact investigations struggle to keep up with the volume and sophistication of financial crime in a hyper-connected world.

The good news? Technology gives us the best opportunity we've ever had to turn the tide – and artificial intelligence (AI) is fast becoming a critical part of that fight.

The Case for Technology — and Why AI Matters

For as long as there's been money, there have been people trying to steal it, hide it, or move it in ways they shouldn't. What has changed, however, is the velocity and sophistication of these crimes – and the environment in which criminals operate. As financial systems become increasingly interconnected and digital, criminals have found new ways to exploit vulnerabilities and conceal illicit activity.

Fortunately, technology offers us our most powerful set of tools yet to fight back. Innovations in real-time monitoring, data analytics, blockchain forensics, and biometric verification have already transformed parts of the compliance landscape. But one area still often misunderstood – or met with caution – is artificial intelligence (AI).

AI isn't a futuristic novelty reserved for big tech firms or experimental labs. It's a practical, proven technology that's already enhancing financial crime detection and prevention in real-world environments. And for compliance teams, it represents an opportunity to work smarter, focus resources more effectively, and proactively manage risk.

From Reactive to Proactive

Historically, financial crime detection has been reactive. Suspicious transaction alerts would trigger after the fact, investigators would follow paper trails, and compliance teams would manually sift through data. It was time-consuming, fragmented, and often ineffective against modern, high-speed financial crime.

Today's technology allows firms to move from reactive monitoring to proactive, intelligence-led financial crime prevention. Real-time transaction monitoring, biometric verification, blockchain analytics, and secure data-sharing platforms are transforming how financial institutions and regulators respond.

Where AI Fits In

AI strengthens this technological shift in meaningful ways. It enhances existing systems by processing vast amounts of data faster than any human could, identifying complex patterns, and surfacing hidden risks.

AI is already proving its value in areas such as:

- Transaction Monitoring Optimisation: AI can detect subtle anomalies in transaction behaviour – spotting unusual patterns that rules-based systems miss, while reducing false positives.
- Network Analysis: Criminal networks often disguise illicit activity by spreading transactions across accounts, jurisdictions, and asset types. AI-powered tools can map connections between entities, transactions, and locations, revealing hidden networks and suspicious relationships.

- Document and Data Review: AI can rapidly process unstructured data – from company filings to emails and adverse media – flagging potential risks and inconsistencies during customer due diligence or investigations.
- Fraud Detection: In payments, AI models can detect fraud in real time, identifying unusual activity patterns before funds leave an account.
- Sanctions and Watchlist Screening: Natural language processing (NLP) tools can help match names against complex sanctions lists more accurately, accounting for spelling variations, aliases, and contextual clues.

Demystifying AI in Financial Crime Compliance

Much of the hesitation around AI stems from misconceptions: that it's a black box, that it will replace human jobs, or that regulators won't accept AI-driven decision-making.

In reality:

- AI is an enhancer, not a replacement. It processes vast amounts of data at speed, identifying patterns and anomalies humans might miss – but it still relies on human oversight and expertise to interpret results and make final decisions.
- It reduces noise, not transparency. Modern AI tools are increasingly explainable, with regulators actively encouraging innovation in financial crime controls, provided firms can evidence how AI models operate and manage risks like bias or error.
- It's already in use. Many firms are already applying AI in areas such as sanctions screening, transaction monitoring optimisation, and adverse media review. What's new is the scale and maturity of these tools, making them accessible to firms of all sizes.

Empowering, Not Replacing, Human Expertise

One of the most promising developments in AI is the rise of agentic workflows – task-oriented systems that can operate semi-autonomously within clearly defined guardrails. These AI agents can support time-intensive tasks such as data collation, alert triage, or preliminary risk assessments, helping to streamline workflows without displacing human oversight. Crucially, they are not decision-makers – they are decision-support tools.

Used responsibly, AI agents free up skilled professionals to focus on what matters most: applying judgement, interrogating context, and making complex ethical decisions. AI agents can extend human capability.

As these tools become more widely available, the real challenge – and opportunity – for compliance leaders is not whether to adopt AI, but how to do so in a way that reinforces governance, safeguards fairness, and embeds accountability from the start. Avoidance is not a risk-mitigation strategy. Engagement is.

An Opportunity, Not a Threat

AI isn't here to take over compliance functions; it's here to make them more effective, efficient, and resilient. By embracing AI thoughtfully and responsibly, compliance professionals can move from reactive processes to proactive risk management – focusing their expertise where it matters most, while technology handles the heavy lifting.

The financial crime landscape has already changed. The question is no longer whether to adopt AI, but how to do it in a way that strengthens your control framework, satisfies regulators, and better protects your business and customers.