CASE STUDY

FIGHTING TECH-FUELED CRIME

Chady El Khoury

The Department of Justice in June announced the largest-ever US crypto seizure: $225 million from crypto scams known as pig butchering, in which organized criminals, often across borders, use advanced technology and social engineering such as romance or investment schemes to manipulate victims. This typically involves using AI-generated profiles, encrypted messaging, and obscured blockchain transactions to hide and move stolen funds.

It was a big win. Federal agents collaborated across jurisdictions and used blockchain analysis and machine learning to track thousands of wallets used to scam more than 400 victims. Yet it was also a rare victory that underscored how authorities often must play catch-up in a fast-changing digital world. And the scammers are still out there.

Criminals are outpacing enforcement by adapting ever faster. They pick the best tools for their schemes, from laundering money through crypto and AI-enabled impersonation to producing deepfake content, encrypted apps, and decentralized exchanges. Authorities confronting anonymous, borderless threats are held back by jurisdiction, process, and legacy systems.

Annual illicit crypto activity growth has averaged about 25 percent in recent years and may have surpassed $51 billion last year, according to Chainalysis, a New York–based blockchain analysis firm specializing in helping criminal investigators trace transactions.

Bad actors still depend on cash and traditional finance, and money laundering specifically relies on banks, informal money changers, and cash couriers. But the old ways are being reinforced or supercharged by technologies to thwart detection and disruption.

Authorities must keep up and respond urgently as digital tools accelerate financial crime

Encrypted messaging apps help cartels coordinate cross-border transactions. Stablecoins and lightly regulated virtual asset platforms can hide bribes and embezzled funds. Cybercriminals use AI-generated identities and bots to deceive banks and evade outdated controls. Tracking proceeds generated by organized crime is nearly impossible for underresourced agencies.

AI lowers barriers to entry. Fraudsters with voice-cloning and fake-document generators bypass the verification protocols many banks and regulators still use. Their innovation is growing as compliance systems lag. Governments recognize the threats, but responses are fragmented and uneven—including in regulation of crypto exchanges. And there are delays implementing the Financial Action Task Force's (FATF's) "travel rule" to better identify those sending and receiving money across borders, which most digital proceeds cross.

Meanwhile, international financial flows are increasingly complicated by instant transfers on decentralized platforms and anonymity-enhancing tools. Most payments still go through multiple intermediaries, often layering cross-border transactions through antiquated correspondent banks that obscure and delay transactions while raising costs. This helps criminals exploit oversight gaps, jurisdictional coordination, and technological capacity to operate across borders, often undetected.

Safe payment corridors

There's a parallel narrative. Criminals exploit innovation for secrecy and speed while companies and governments test coordination to reduce vulnerabilities and modernize cross-border infrastructure. At the same time, technological implications remain underexplored with respect to anti–money laundering and countering the financing of terrorism, or AML/CFT.

Singapore's and Thailand's linked fast payment systems, for example, enable real-time retail transfers using mobile numbers; Indonesia and Malaysia have connected QR codes for cross-border payments. Such innovations offer efficiency and inclusion yet raise new issues regarding identity verification, transaction monitoring, and regulatory coordination (see "Southeast Asia's Cross-Border Payment Push" in this issue of F&D).

In India, the Unified Payments Interface enables seamless transfers across apps and platforms, highlighting the power of interoperable design. More than 18 billion monthly transactions, many across competing platforms, show how openness and standardization drive scale and inclusion. Digital

"Regulators and fintechs should be partners, and sustained multilateral engagement should foster fast, cheap, transparent, and traceable cross-border payments."

payments in India grew faster when interoperability improved, especially in fragmented markets where switching was costly, IMF research shows (see "India's Frictionless Payments" in this issue of F&D).

These regional innovations and global initiatives reflect a growing understanding that fighting crime and fostering inclusion are interlinked priorities—especially as criminals speed ahead. The FATF echoed this concern, urging countries to design AML/CFT controls that support inclusion and innovation. Moreover, an FATF June recommendation marks a major advance: Requiring originator and beneficiary information for cross-border wire transfers—including those involving virtual assets—will enhance traceability across the fast-evolving digital financial ecosystem.

Efforts like these are important examples of how technology enables criminal advantage, but technology must also be part of the regulatory response.

Modernizing cross-border payment systems and reducing unintended AML/CFT barriers increasingly means focusing on transparency, interoperability, and risk-based regulation. The IMF's work on "safe payment corridors" supports this by helping countries build trusted, secure channels for legitimate financial flows without undermining new technology. A pilot with Samoa—where de-risking has disrupted remittances—showed how targeted safeguards and collaboration with regulated providers can preserve access while maintaining financial integrity without disrupting the use of new payment platforms.

Machine learning

Several countries, with IMF guidance, are investing in machine learning to detect anomalies in cross-border financial flows, and others are tightening regulation of virtual asset service providers. Governments are investing in their own capacity to trace crypto transfers, and blockchain analytics firms are often employed to do that.

IMF analysis of cross-border flows and the updated FATF rules are mutually reinforcing. If implemented cohesively, they can help digital efficiency coexist with financial integrity. For that to happen, legal frameworks must adapt to enable timely access to digital evidence while preserving due process. Supervisory models need to evolve to oversee both banks and nonbank financial institutions offering cross-border services. Regulators and fintechs should be partners, and sustained multilateral engagement should foster fast, cheap, transparent, and traceable cross-border payments—anchored interoperable standards that also respect privacy.

Governments must keep up. That means investing in regulatory technology, such as AI-powered transaction monitoring and blockchain analysis, and giving agencies tools and expertise to detect complex crypto schemes and synthetic identity fraud. Institutions must keep pace with criminals by hiring and retaining expert data scientists and financial crime specialists. Virtual assets must be brought under AML/CFT regulation, public-private partnerships should codevelop tools to spot emerging risks, and global standards from the FATF and the Financial Stability Board must be backed by national investments in effective AML/CFT frameworks.

Consistent and coordinated implementation is important. Fragmented efforts leave openings for criminals. Their growing technological advantage over governments threatens to undermine financial integrity, destabilize economies, weaken already fragile institutions, and erode public trust in systems meant to ensure safety and fairness. As crime rings adopt and adapt emerging technologies to outpace enforcement, the cost is not only fiscal—it is structural and systemic. Governments can't wait. The criminals won't. F&D

CHADY EL KHOURY *is an assistant general counsel and a division chief in the IMF's Legal Department.*