Investment Executive

The futile war against high-tech crime

Fraud, scams increasingly powered by AI, tech

May 19, 2026

While the financial industry is eager to exploit the growing power of emerging technologies, fraudsters are already doing it — using technologies such as AI and crypto to supercharge investment scams, an industry conference heard.

Reported losses from fraud and related crimes in the U.S. were up by 26% in 2025 to an estimated US$21 billion, according to data from U.S. Federal Bureau of Investigation (FBI) cited at the U.S. Financial Industry Regulatory Authority Inc.'s (FINRA) annual conference in Washington, D.C.

That increase is being empowered, in large part, by technology.

According to Heith Janke, assistant director, criminal division at the FBI, the rise in fraud is being driven by emerging threats such as crypto scam compounds in Southeast Asia that are engaging in fraud at an industrial scale; increasingly sophisticated cyberattacks, such as account takeover and business email compromise scams, are becoming much more efficient and effective with the power of advanced tools; and fraudulent investment clubs that are assembling over social media.

At the same time, offering frauds and co-ordinated market manipulation schemes are also being made more effective by AI, noted Dan McClain, vice president, surveillance and market intelligence at FINRA.

Press releases that are designed to lure unsuspecting investors to pump-and-dump schemes are more convincing than ever, and the easy hallmarks of scam activity in past years, such as poor spelling and grammar, are disappearing as AI creates content for foreign fraudsters that aren't native English speakers.

In some cases, the likenesses of financial advisors are being used in these kinds of schemes too, the conference heard — with legitimate advisors having their images and voices used in deepfakes to give investment club scams an air of legitimacy.

Indeed, imposter scams involving both industry personnel and regulators are also on the rise, thanks to easily accessible AI tools.

These same capabilities are also being used to improve the social engineering side of scam activity — such as investors being tricked into giving fraudsters access to their accounts by prompting them to reset account passwords — suggested Samantha Larew, chief compliance officer at Manning & Napier Investor Services, Inc.

While the underlying scams themselves aren't necessarily novel, the power of technology is breathing new life into time-worn efforts by criminals to separate investors from their money, the conference heard.

The panellists stressed that the financial industry is on the front lines of much of this activity, and is often the first line of defence in protecting investors — increasing the importance of training, and other industry efforts to combat fraud.

These emerging threats are also raising concerns with regulators in the U.K.

In a joint statement last week, the Financial Conduct Authority (FCA), the Bank of England and HM Treasury warned financial industry firms about the threat posed by "frontier AI" models that "amplify cyber threats to firms' safety and soundness, customers, market integrity and financial stability."

These threats are only expected to increase as the models become more powerful, and the regulators warned that the industry firms will become increasingly vulnerable.

Against that backdrop, they warned that, "It is essential that firms have effective protective, detective, threat containment and cyber response capabilities including to address faster and more disruptive frontier AI-driven attacks."

Among other things, they called on firms to ensure they understand the emerging risks, and have a strategy and the resources required to mitigate them.

“Firms should be able to triage, prioritize, risk assess, and remediate vulnerabilities more quickly, more frequently, and at scale, including through automation where appropriate, while mitigating the operational risks from doing so,” they said. In addition, firms should consider adopting automated defences that can operate at the same speed as AI-powered attacks, and ensure that they are capable of recovering from a successful attack, they said.

At the same time, “Firms should also consider whether they have appropriate insurance in place,” they noted.