MINTZ GROUP

Clarity in a complex world

"The emergence of AI has irrevocably altered the landscape for both fraudsters and those who pursue them."

Staying a Step Ahead of Fraudsters in the Age of AI

by Brooke Berg, Nathan Patin & Eleanor Warnick

This article was originally published in the *ICC FraudNet Global Annual Report 2025* entitled "The State of Fraud and Asset Recovery: Timeless Crimes, Modern Approaches."

If AI is revolutionizing banking, finance and commerce, it is having the same dramatic effect in the underworld, giving bad actors powerful new capabilities and amplifying the harm they can inflict. For example, AI is enabling fraudsters to create convincing emails that appear to be from banks or payroll departments for use in phishing attacks. Fraudsters are also using AI-powered voice cloning to impersonate executives, bank representatives or even family members in real-time phone scams, tricking victims into transferring money or disclosing sensitive information. AI's ability to automate transactions and quickly generate legitimate-seeming invoices and contracts makes money laundering harder to detect. Investment scams are made more convincing through deep-faked news articles and celebrity endorsement videos.

Perhaps most importantly, AI-driven fraud makes it easy for bad actors to cast a wider net, significantly expanding the pool of organizations and individuals at risk of becoming threat targets. Phishing scams, for example, are no longer labor-intensive; AI can now generate and personalize them at scale. As a consequence, rather than focusing on large organizations—which generally can be counted on to have sophisticated defenses—bad actors can now profitably target a large number of smaller, and possibly more vulnerable, entities.

Looking beyond an AI Arms Race

Naturally, investigators and others charged with risk mitigation, fraud detection and asset recovery have responded in kind, developing AI-driven tools and approaches to monitor threats and ferret out malfeasance. But the new threat landscape requires more than keeping up in a technological arms race. When AI has given fraudsters the ability to move quickly, obfuscate with mounds of data and generate fake identities, investigators must double down on three traditional imperatives: speed and accuracy, differentiating signal from noise, and identification and disambiguation. While these capabilities have always been important, they are now the central pillars of investigative work, and the processes used by investigators must evolve accordingly.

For example, a large category of investigative work involves combing through troves of data to extract patterns, as when a case requires slogging through thousands of dense U.S. Securities and Exchange Commission (SEC) filings in an effort to identify a subject's holdings for asset recovery. Historically, this has required a brute-force approach, constructing elaborate spreadsheets to map transactions or connections between entities. Now, however, AI-powered tools that have been appropriately trained can conduct such analysis almost instantaneously, not just mapping holdings and fund flows, but uncovering ultimate beneficial ownership.

AI also makes it possible to identify patterns in much larger datasets, such as those generated by social media. Recently, for example, we were asked to help identify the distributors of counterfeit Covid home testing kits. We realized that social media posts about the product created a map of the product's end users; we were able to use an AI-powered tool to reverse-engineer the distribution chain to help point to the source of the counterfeit goods.

AI-powered social media analysis is also useful when high-profile disputes play themselves out online. In such conflicts, it is important to know how much of the venom is the organic by-product of vocal supporters taking sides and how much might be due to a smear campaign orchestrated by the opposition. Hours of podcasts and YouTube videos can be automatically transcribed and analyzed for tell-tale clues; other tools can then analyze those transcripts and social network traffic to identify key influencers, who can then be scrutinized to see if they are linked to troll farms. Similarly, AI tools can be used to see if online attacks on brands are being initiated by competitors or other economically motivated actors, or to help distinguish genuine threats from background chatter in cases of ongoing online harassment.

In addition to accelerating the investigative process and separating signal from noise, AI tools are also enabling investigators to enhance identification and disambiguation. In one recent case, we were asked by the administrator of a professional credentialing exam to help crack an online cheating ring operating on a Discord server. While the ring members all used aliases, we were able to link one member to an anonymized online account in which he had posted a photo of himself—but in which his face was pixelated. But just as AI tools can create fake images, they can also unscramble digitally-altered photos. While we couldn't do so perfectly, it was enough to allow a second AI platform to help us identify the subject in the photo.

New Possibilities Demand New Approaches

These case studies illustrate the range of ways in which AI can be harnessed to make investigations faster and more effective. But these examples also highlight important principles underlying the use of AI. First, while AI provided the critical capabilities in each of these cases, AI is only a tool that is as effective as the investigators using it. AI platforms thus operate best when they are essentially virtual members of an experienced investigative team: AI-generated insights provide a foundation that investigators then refine through experience, intuition and contextual knowledge. The effective use of AI thus depends on its effective integration into the investigative workflow.

Second, cutting-edge application of AI requires investigators and others on the front lines to think more broadly about data and information. Using AI to extract information about named entities in piles of SEC reports is a fairly straightforward use case. But to use AI to construct influencer networks from social media data, it helps to have a basic understanding of network structure. To be sure, as new uses of AI become standard practice, it will be less necessary to grasp the theoretical underpinnings of various AI use cases. But broader awareness allows one to be at the forefront of what is possible.

Finally, investigations firms need to adopt a stance of constant evolution with respect to AI. In some ways, investigations and AI are now in a position similar to that of the internet and the publishing industry at the beginning of this century—the technology is moving from the periphery to the center and gaining speed in doing so. The disruptions of the internet forced publishers to not just re-center their product and its distribution, but to reimagine what was possible. Similarly, in the face of the rapid evolution of AI, investigators are having to evolve their processes and workflow to match a new vision of what it means to extract true knowledge from mere data.

The emergence of AI has irrevocably altered the landscape for both fraudsters and those who pursue them. The same technological advances will be available to both sides. The advantage, then, is likely to lie with whomever can best adapt to the changes that AI brings.

Brooke Berg
Director
Washington, D.C.
Office: +1 202 887 9100
bberg@mintzgroup.com

Nathan Patin
Director, Head of Digital Investigations
Washington, D.C.
Office: +1 202 887 9100
npatin@mintzgroup.com

Eleanor Warnick
Director
London
Office: +44 20 3137 7004
ewarnick@mintzgroup.com