AI and Fraud: Fighting Fire with Fire

By **David Elzinga**, FCPA, FCA•IFA, CFE
Senior Director, Delta Consulting Group

The emergence of artificial intelligence (AI) has significantly streamlined investigative work by reducing the burden of repetitive and time-consuming tasks. Where investigative teams once devoted months to manually reviewing and cataloguing dozens or sometimes hundreds of boxes of discovery materials, digital forensics and e-discovery tools now allow those same records to be processed, organized and analyzed electronically in a fraction of the time. This transformation has not only accelerated document review but also enhanced accuracy, accessibility and collaboration in complex investigations.

As technology advances past the more commonplace e-discovery tools, AI is now also being touted as a powerful shield against financial and occupational fraud. Not only can AI models monitor transactions as they are occurring and flag anomalies instantly, but machine learning means the systems can continuously evolve to keep up with new fraud tactics. Private companies and public sector organizations have hastened to implement AI-based fraud detection tools, reporting significant savings and recoveries annually. Additionally, AI-based fraud detection tools report fewer false positives compared to older systems, improving operational efficiency.

But there’s a flipside: fraudsters are using AI too, and the result is an escalating arms race, in which businesses and criminals are constantly trying to outsmart each other.

In a December 2024 public service announcement issued by the Federal Bureau of Investigation (FBI), the U.S. government warned individuals and organizations about the ways that criminals are using generative AI to scale fraud and increase believability, reducing time/effort to deceive victims. And the United Kingdom’s National Cyber Security Centre assesses that AI is increasing the scale and success rate of phishing and social-engineering, lowering the barrier for less-skilled criminals, suggesting an elevated risk outlook through 2027.

Awareness of evolving fraud schemes is one of the most effective mitigants for organizations to reduce risk. Here are some of the most common ways that perpetrators are using AI to achieve their goals.

IDENTIFYING AND EXPLOITING SYSTEM WEAKNESSES

Fraudsters can use AI to probe firewalls, and internal controls to find weaknesses and trick fraud detection models by scanning public assets, looking for open "doors" in your system, scraping employee profiles and trying many attack permutations. Rather than a human manually probing a target over days or weeks, an AI agent can try thousands of password guesses or variants; and then iteratively refine attacks based on what succeeds.

BOT-POWERED FRAUD

Leveraging AI to mimic human interactions, fraudsters can scale up scams like romance fraud and investment fraud to maintain long conversations, launch credential-stuffing attacks, or simulate human behavior to evade detection.

QUANTUM THREAT TO ENCRYPTION

As quantum computing advances, it is expected to render current encryption methods like RSA and ECC vulnerable to rapid decryption, exposing confidential data and financial systems. Organizations must begin transitioning to **post-quantum cryptography** to safeguard against future large-scale breaches and AI-accelerated fraud.

PHISHING AND SOCIAL ENGINEERING

Generative AI enables hyper-personalized phishing emails, texts and calls that mimic real people and organizations.

DEEPFAKES & SYNTHETIC IDENTITIES

Using the same methods companies are using for identity verification, fraudsters are using facial recognition software, voice analysis and document verification to generate fake videos, voices and documents to bypass authentication systems.

In a striking case of AI-enabled fraud, a finance employee at global engineering firm was tricked into transferring $25.6 million after joining a video call with what appeared to be the company's CFO and colleagues. In fact, they were all AI-generated deepfakes. Attackers used publicly available video and audio to create realistic replicas of executives, convincing the employee to authorize multiple transfers. The incident shows how generative AI can make social-engineering scams alarmingly convincing, even to experienced professionals, and highlights the urgent need for fraud-prevention strategies that address AI-driven deception.

The news isn't all negative. Just as bad actors seek to exploit AI for nefarious purposes, AI can also be a powerful ally in the fight against fraud. AI fraud prevention tools can search millions of records in seconds and highlight the highest-risk cases, so investigators spend time where it matters most. AI tools can build maps showing connections between people, accounts and companies. And AI can 'tell on itself,' catching AI-generated images, documents or voices that might otherwise pass as real to us.

Ultimately, there is a delicate balance between using emerging technology in concert with human judgment. While AI can make fraud detection faster, smarter, and more efficient, no system is foolproof. Human expertise and experience with fraud schemes is still critical and you must be vigilant to ask tough questions, spot inconsistencies and navigate human behavior in ways machines cannot.

Fraudsters will not stop innovating, and neither can investigators. AI is not magic, but it is an essential part of the modern fraud-fighting toolkit. The key is balance: combining advanced technology with the experience and intuition that only people can bring to problems.

ABOUT THE AUTHOR

DAVID J. ELZINGA, FCPA, FCA•IFA, CFE

SENIOR DIRECTOR

T: +1 403-261-2181 E: delzinga@delta-cgi.com

David J. Elzinga, FCPA, FCA•IFA, CFE, has served as an expert testifier and forensic investigator for over 30 years, representing clients on matters involving economic losses, criminal fraud and secret commissions, money laundering, insurance investigations, breach of contracts, shareholder disputes, family law matters, special purpose audits, and security related issues.