ALERT

Fraud and Scam Prevention Series: Navigating Increasingly Sophisticated Cybersecurity Threat and Fraud Tactics

November 12, 2025

Cybersecurity risks are evolving, in part because bad actors – including scammers and fraudsters – are leveraging widely available artificial intelligence (AI) tools for nefarious purposes. In the escalating fraud landscape, companies should be attuned to emerging risks and should consider adjusting their reasonable cybersecurity and anti-fraud practices to keep pace.

The Federal Bureau of Investigation's (FBI) April 2025 Internet Crime Report estimated losses exceeding $16 billion from internet crime in 2023. The financial consequences of cybersecurity incidents can be significant for organizations; the average total cost of a data breach in the U.S. has been estimated at $9.36 million. High-profile incidents, such as the theft of hundreds of millions of customer records from large corporations, underscore the scale of this threat. While sophisticated zero-day exploits may grab headlines, criminals and fraudsters continue to exploit employees through phishing and the use of stolen or compromised credentials – and the use of AI tools enables those bad actors to find more potential targets and move faster to exploit them.

Bad-Actor Adoption of AI Is Fueling Next-Generation Fraud

The fraud landscape is evolving at an unprecedented pace, driven by rapid technological advancements. What was once limited to basic data theft has transformed into highly orchestrated, targeted deception that exploits complex systems and human behavior. A range of financially motivated actors use phishing, various extortion or ransomware schemes, and other cyber-enabled methods such as

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kevin G. Rupy
Partner
202.719.4510
krupy@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
lbrown@wiley.law

Joshua K. Waldman
Associate
202.719.3223
jwaldman@wiley.law

Alissa Lynwood
Associate
202.719.4527
alynwood@wiley.law

Practice Areas

Artificial Intelligence (AI)

Cyber and Privacy Investigations, Incidents & Enforcement

Federal Policy and Regulation

Litigation

Privacy, Cyber & Data Governance

State Regulation

Telecom, Media & Technology

call center or tech support scams. Businesses that recognize this shift can take proactive steps to strengthen defenses to stay ahead of increasingly intelligent and adaptive threats, such as the ones outlined below.

- Using AI to Generate Cybersecurity Threats: Cyber threat actors, including financially motivated ones, are using AI tools across multiple stages of the attack cycle, including scanning potential targets, creating or delivering malware, and even vulnerability research.
- Creation of Fraudulent Identities: Fraud schemes often rely on convincing the victim that the perpetrator is a trusted, authentic actor – and fraudsters are increasingly using AI to fool victims. The U.S. Department of the Treasury Financial Crimes Enforcement Network (FinCEN) has described in an alert how fraud schemes are using AI to "circumvent identity verification and authentication methods." Fraudulent actors have used AI to alter or generate images used for identification documents, such as driver's licenses or passports, in order to bypass financial institutions' onboarding and know-your-customer protocols. Those bad actors have gone on to engage in check fraud, loan fraud, and credit card fraud.
- Remote Worker Fraud: AI use by cybercriminals has even facilitated fraudulent work schemes targeting the technology sector, including one organized effort in which the proceeds went back to North Korea, as we noted earlier this year. Those criminals used AI to enhance photos for false identity documents.

Businesses and Organizations Need Comprehensive Strategies to Combat Fraud

Cybersecurity is not just an IT problem – nor is financial fraud an issue solely for loss-prevention or fraud teams. Mitigating fraud can be part of an organization's operational resilience practices. As fraud tactics grow more sophisticated, businesses and organizations should evaluate vulnerabilities in their networks and systems and implement layered security measures to protect against fraud, including AI-powered fraud. Organizations should review data collection and storage processes to protect against exploitation by advanced fraud schemes. Best practices for businesses and organizations to consider include the following:

1. Prioritize Cyber Hygiene: For both individuals and organizations, core cybersecurity practices are an important defense against internet-enabled fraud. The Cybersecurity & Infrastructure Security Agency (CISA) emphasizes that cyber hygiene includes timely software updates; using strong, unique passwords; and turning on multi-factor authentication for critical systems. As the National Institute of Standards and Technology (NIST) has identified, because AI capabilities can also help bad actors generate new schemes and tactics while also making it easier to exploit existing capabilities, organizations may need to adapt their defenses. Organizations can consider, for example, expanding awareness and training activities to specifically address AI-enabled social engineering.
2. Data Minimization Can Mitigate Risk: Data minimization can be an important part of the equation for protecting data from sophisticated fraud schemes. The unnecessary accumulation of data increases the exposed attack surface, offering cybercriminals an enticing target should a security incident occur. Appropriate data minimization and data retention practices can supplement data protection, which uses technical measures like encryption and access controls to secure the data an organization is legally or operationally required to hold. By applying reasonable data minimization and retention principles, organizations can help to reduce the attack surface and mitigate the increasing financial and legal risks posed by the current fraud environment.
3. Sharing Information Across Disciplines: Organizations should also look for ways to increase collaboration among key parts of an organization, including cybersecurity professionals, fraud prevention, and finance teams, who are in a position to monitor and catch financial fraud like misdirection of funds. The Cybersecurity Information Sharing Act of 2015 (CISA 2015) (which expired in September 2025) promoted the development of Information Sharing and Analysis Centers and established a framework for sharing at scale of cyber threat indicators and defensive measures. However, as some commentators have noted, the law authorized and promoted sharing of a relatively limited set of technical data. Broader, richer information about scam tactics and perpetrators may not have been fully covered by CISA 2015, leading some to call for more robust cross-sector information exchange of scam intelligence. And while that infrastructure may take time to build, companies can promote cross-functional sharing of cyber and financial fraud threat information within their own organizations by formalizing collaboration between cybersecurity and fraud prevention personnel.
4. Follow the Money: Cybercriminals often rely on fooling victims into transferring funds to what they believe are legitimate vendor or customer accounts, which means that an organization's procurement, financial, and accounting teams are the front lines of defending against these activities. Companies should also consider reviewing their policies and payment authentication and verification procedures, especially procedures around changing payment methods or destinations, to mitigate risks from potentially fraudulent payments or funds transfers.

AI-driven and cyber-enabled fraud is advancing at a speed that leaves little room for complacency. Companies and organizations should consider proactive, holistic strategies to safeguard their data, systems, and customers. The cost of inaction is steep – those who fail to act now risk falling victim to the next wave of intelligent, adaptive threats. Please stay tuned for our next article in this Fraud and Scam Prevention Series.

***

Wiley has a deep and experienced multidisciplinary team, and our experts handle a broad range of complex legal and policy issues in the fraud environment. From creative litigation strategies that take down scammers, to effective regulatory advocacy across multiple federal agencies, Wiley attorneys have extensive knowledge of today's fraud environment. Wiley advises on all aspects of the cyber incident lifecycle, from readiness to response to resilience and continuity. We have decades of experience in cybersecurity preparedness, intrusion and law enforcement investigations, regulatory inquiries or enforcement actions, government liaison, data breach and data governance issues, crisis management, strategic communications, and business disaster recovery matters. For more information or assistance, please contact one of the authors listed on this alert.