AI: A Double-Edged Sword in the Fight Against Identity Theft and Fraud

January 14, 2025 - Artificial intelligence is reshaping the fight against identity fraud in the United States, but it's also fueling a disturbing rise in sophisticated scams. As AI tools become more powerful and accessible, both criminals and corporations are using them - but for very different ends.

According to a new report from Experian, consumers lost $12.5 billion to fraud in 2025, a staggering figure that's expected to climb in 2026 as AI-powered scams gain traction. These scams often include voice cloning, deepfake videos, and phishing emails so convincing they can fool even the most cautious consumers. Impersonation scams - where fraudsters pose as trusted individuals or organizations - rose 148% last year and are now the most common type of fraud. AI is giving scammers tools that once seemed like science fiction. Cybercriminals can now automate scam operations, create realistic fake identities, and even simulate live conversations. As a result, financial institutions, retailers, and consumers are facing a wave of fraud that's harder to detect and more damaging when successful.

But AI is also at the center of the response. Banks, credit monitoring services, and online platforms are increasingly turning to machine learning and artificial intelligence to detect unusual activity, verify user identities, and prevent fraud in real time. A recent survey found that more than a third of U.S. businesses are using AI-based fraud detection tools, and many are investing heavily in new security technologies.

This tug-of-war between criminal innovation and corporate defense is reshaping the digital economy. While AI makes it easier for companies to spot anomalies and alert users to potential breaches, it also gives criminals the same power to learn, adapt, and deceive.

Synthetic identity fraud, where fake personas are built from a combination of real and fictitious information, is one example of this complexity. Experts estimate losses tied to synthetic identities could top $30 billion in 2026. These fake profiles often bypass traditional security checks, making them difficult to detect until it's too late.

Consumers are increasingly anxious. A recent national survey found that 85% of Americans believe AI has made scams harder to spot. In response, agencies like the Federal Trade Commission and cybersecurity experts are urging people to be cautious with personal information, use multi-factor authentication, and remain skeptical of unsolicited communications.

As artificial intelligence continues to evolve, so will the threats and defenses surrounding identity theft. For now, the technology remains a double-edged sword - an incredible asset in the hands of protectors, and a dangerous weapon when wielded by criminals.

by Jim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS