NICE Actimize

Insights Article

AI in the Hands of Fraudsters: A New Era of Digital Deception

How Criminals Are Weaponizing Artificial Intelligence to Defraud the Financial System

By Chen Ari Kirsch, Fraud Prevention Subject Matter Expert

Artificial Intelligence (AI) has transformed industries across the globe, delivering efficiencies, insights and automation at an unprecedented scale. As with any powerful technology, AI is a double-edged sword. While it has advanced fraud defense capabilities and strategies, it has also empowered fraudsters with new tools and opportunities to exploit. From synthetic identities to deepfake impersonations, fraudsters now wield AI to scale deception, bypass controls and exploit trust. In this article, we'll explore how AI is reshaping the fraud landscape, emerging as both a powerful tool for prevention and a potent weapon for fraudsters, with real-world examples that highlight the urgency of this growing threat.

Synthetic Identities and Money Mule Networks

One of the most concerning applications of AI in fraud is the creation of **synthetic identities**—fake personas built using a combination of real and fabricated data. Traditionally, fraudsters would manually stitch together stolen Social Security numbers, addresses and names. Today, AI can automate this process efficiently and at scale.

Generative models can produce realistic names, photos and even social media profiles that pass basic verification checks. These synthetic identities are then used to open bank accounts serving as **money mule accounts**—intermediaries that move illicit funds across borders.

What makes this particularly dangerous is the ability of AI to simulate behavioral patterns. Fraudsters can train bots to mimic legitimate user activity, making these accounts appear authentic to fraud detection systems. This undermines traditional Know Your Customer (KYC) controls and makes it harder for financial institutions to distinguish real customers from AI-generated imposters.

New data from Sumsub has claimed that the creation of fake documents using AI grew by 195% worldwide between Q1 2024 and Q1 2025. The most dramatic spike was recorded in Europe, where synthetic ID fraud surged by 378%, followed by North America (311%) and the MENA region (258%).

Multi-Language Phishing Campaigns

Phishing has long been a staple of fraud, going back centuries, whether it be the "Spanish prisoner" letters or "Nigerian prince" emails. AI, however, has elevated it to a global scale. Previously, language barriers limited fraudsters to targeting victims in their native tongue. Now, AI-powered translation tools and natural language generation models allow fraudsters to craft convincing phishing emails in dozens of languages, expanding their target pool. This also enables fraud rings to centralize operations in low-cost regions while targeting high-value victims globally.

These emails are no longer riddled with grammatical errors or awkward phrasing. Instead, they read fluently, mimic local idioms and even replicate the tone of legitimate communications from banks, government agencies and employers.

For example, a fraudster targeting a multinational company can now send tailored phishing emails to employees in Germany, Brazil and Japan—all in their native languages, with culturally appropriate messaging. This dramatically increases the success rate of phishing campaigns and expands the reach of fraud operations.

As an example, the **Darcula phishing platform** sells "phishing as a service" (PhaaS) using AI to generate multilingual phishing websites and messages, targeting victims globally with convincing brand impersonations.

Real-Time Language Translation for Phone-based Social Engineering

Social engineering over the phone has traditionally required fluency in the target's language. AI has removed that barrier. With **real-time language translation tools**, fraudsters can now engage victims in live conversations, translating speech on the fly.

Imagine a scammer in a non-English speaking country calling a victim in London. Using AI-powered translation, they can understand and respond in English, even if they don't speak a word of it. This opens the door to impersonation scams, tech support fraud and vishing (voice phishing) attacks across linguistic boundaries.

Moreover, AI can help fraudsters adapt their tone and vocabulary based on the victim's responses, making the interaction feel more natural and trustworthy. This dynamic manipulation of language is a powerful tool for psychological exploitation.

Voice and Face Emulation for Deepfake Social Engineering and Identity Circumvention

Perhaps the most chilling development is the use of **deepfake technology** to emulate voices and faces in real time. Fraudsters can now clone a person's voice using just a few seconds of audio. With video, they can generate realistic facial animations that mimic expressions, lip movements and gestures.

These attacks are not theoretical, they've already occurred. In one high-profile case, An employee in Hong Kong was tricked into wiring $25 million after attending a video call with deepfake versions of his colleagues. In a different case, fraudsters used an AI-generated voice to impersonate a company executive and trick an employee into transferring $243,000.

These attacks are particularly dangerous in banking environments where video conferencing is used for high-value transaction approvals or identity verification.

AI-Powered Reconnaissance and Targeting

Beyond impersonation and phishing, AI is also used for pre-fraud **reconnaissance**. Fraudsters deploy machine learning algorithms to scan social media, public records and data breaches to build detailed profiles of potential victims.

These Profiles Include:

Employment history

Family relationships

Financial status

Online behavior

Armed with this data, fraudsters can craft highly personalized attacks. For example, they might reference a recent job change or a child's name in a phishing email, increasing the likelihood of engagement. This enables spear-phishing and social engineering attacks that are nearly indistinguishable from legitimate interactions. AI enables this level of targeting at scale, turning what was once manual research into automated exploitation.

Fake Merchants with AI-Generated Backstories

Another emerging tactic involves fraudsters setting up **non-existent merchants**, complete with AI-generated photos, branding and fabricated backstories. These fake businesses are often listed on e-commerce platforms, social media or even payment gateways, appearing legitimate to unsuspecting customers and financial institutions.

In one instance, fraudsters created a fake luxury goods store with AI-generated product images and staff bios. Customers placed orders and paid via card or bank transfer for goods that never existed. The merchant vanished after collecting thousands in payments.

Similarly, a fake travel agency used AI to generate scenic photos, customer testimonials and even a virtual tour guide. Victims booked holidays that were never real, losing deposits and travel funds.

These schemes are particularly dangerous because they exploit trust in digital storefronts and payment systems. AI allows fraudsters to build convincing merchant profiles at scale, making it harder for platforms to detect and remove them before damage is done.

Evading Detection with Adversarial AI

Fraud detection systems themselves often rely on AI-but fraudsters are fighting fire with fire, using **adversarial AI** to test and refine their tactics to evade detection.

One tactic involves simulating thousands of transactions to uncover the patterns that trigger fraud alerts, and then fine-tuning behavior to stay just below those thresholds. This cat-and-mouse game is increasingly automated, with fraudsters using AI to probe defenses and adapt in real time.

This AI arms race between attacker and defender is reshaping the future of fraud detection.

Looking Forward

As a fraud prevention expert, I believe we've only seen the **initial wave** of AI-enabled fraud. The tools available today—synthetic identities, deepfakes, real-time translation—are just the beginning. As AI models become more powerful and accessible, we can expect fraud to evolve in **unexpected and unprecedented ways**.

Future Threats May Include:

Autonomous fraud bots that operate without human oversight

AI-generated fake news campaigns to manipulate markets

Real-time manipulation of financial data or dashboards

The challenge for fraud prevention professionals is to stay ahead of this curve. We must invest in **AI-driven defenses**, enhance **domestic and cross-border collaboration** and rethink **identity verification** in a world where seeing and hearing are no longer believing.

Conclusion

AI is enabling a growing range of sophisticated fraud tactics, from AI driven account takeovers (ATO) and LLM-powered fraud scripting to enhanced invoice and document manipulation, as well as insider threats fueled by AI capabilities. AI is transforming fraud from a manual, opportunistic endeavor into a scalable, strategic operation. It empowers fraudsters to cross borders, languages and trust barriers with ease. As defenders, we must recognize that the threat landscape is no longer static but dynamic, intelligent and rapidly evolving.

The future of fraud is AI-powered, and unless we counter it with equal innovation, vigilance and collaboration, we risk falling behind.

Explore the Industry's Most Powerful AI-Driven Fraud Management Platform

About NICE Actimize

As a global leader in artificial intelligence, platform services, and cloud solutions, NICE Actimize excels in preventing fraud, detecting financial crime and supporting regulatory compliance. Over 1,000 organizations across more than 70 countries trust NICE Actimize to protect their institutions and safeguard assets throughout the entire customer lifecycle. With NICE Actimize, customers gain deeper insights and mitigate risks. Learn more at www.niceactimize.com.