HOW AI STRENGTHENS FRAUD DETECTION.

Fraud is evolving. Your defenses should too.

Fraudsters are now using generative AI to industrialize their attacks: building fake identities, automating phishing campaigns, deploying deepfakes, and scaling social engineering with unprecedented precision. The result? Scams are more convincing, attacks are more coordinated, and financial institutions face a new level of threat—at speed and at scale.

The Shift in Tactics: Smarter, Faster, Harder to Detect

Traditional defenses—based on static rules and known patterns—can't adapt quickly enough to this new wave of AI-enhanced fraud. Attackers use machine learning to avoid detection, natural language models to mimic real customers or support agents, and voice or video deepfakes to impersonate trusted individuals. The human element is weaponized, and trust becomes the entry point.

The Scale of the Threat: Industrialised, Automated, and Always On

AI has enabled fraud to become scalable, borderless, and continuous. Criminal networks now deploy automated scam infrastructures that operate 24/7—constantly refining their tactics, testing for vulnerabilities, and launching thousands of attack variations at once. The low cost of generative AI tools means bad actors can launch convincing attacks with minimal resources, increasing the volume and sophistication of fraud across all channels.

High-risk fraud patterns
AI-enabled scams contributed to over $4B in estimated global fraud losses in 2024. (Restackio)

AI-driven fraud prevalence
AI-driven fraud now constitutes 42% of all detected fraud attempts in the financial sector. (Signicat)

Deepfake Scams
25% of executives faced one deepfake-related scams targeting financial data in 2024. (Incode)

Deepfake CEO Fraud

Fraudsters use deepfake technology to impersonate company executives through AI-generated voice or video. They create convincing messages urging staff to make urgent payments to fraudulent accounts. Employees, believing the request is genuine, act quickly—often before verifying. These scams are difficult to detect and can result in substantial financial losses before being discovered.

AI-Powered Scam Calls

AI is used to create highly personalized phishing emails and voice calls that appear to come from trusted sources. Messages mimic writing style or tone, while robocalls use AI to sound like real agents. Victims are tricked into revealing sensitive data, making the attack seem legitimate until the fraud is complete.

STOP SCAMS IN REAL TIME WITH AI-DRIVEN INTELLIGENCE.

ThreatMark's **Behavioral Intelligence Platform** is built on behavioral intelligence and real-time analysis, enabling banks to detect and disrupt fraud earlier, with greater precision and less customer friction.

Why AI is Essential Against Modern Scams

Social engineering fraud is hard to detect because it manipulates the customer, not the system. These attacks exploit trust and emotion, making traditional fraud controls ineffective. AI helps uncover signals of manipulation—like behavioral anomalies and coerced activity—before damage occurs. ThreatMark's AI detects these patterns in real time, helping banks act early and shift from reactive to proactive fraud prevention.

70%
Better detection rate
(than traditional FDS)

90%
Fewer false positives
(than traditional FDS)

90%
Decrease in cost for authentication
(ets. SMS cost saving)

2
Weeks to implement
(cloud option)

Improved detection & scoring methods
(when integrating with existing systems)

AI in Action: Key Use Cases

ThreatMark's AI doesn't just react—it anticipates. By continuously learning from real-world behavior, device usage, and transaction context, it builds a dynamic risk picture of each user. This allows financial institutions to detect fraud patterns early, act decisively, and protect customers without adding friction.

Behavioral Profiling
AI analyzes user behavior across sessions, detecting inconcsistencies that indicate fraud such as bot-driven transactions or social engineering attacks.

Early Warning System
Predicts and prevents fraud by identifying subtle risk indicators, such as unusual payment patterns, sudden device changes, or scammer-controlled activity.

Reducing False Positives
Machine learning refines risk scoring, ensuring genuine customers aren't blocked while fraudsters are stopped before money is moved.

Detecting Social Engineering Scams
AI indentifies manipulation tactics like live call coaching, RAT activity, or coerced transactions, altering banks before funds are lost.

Protecting Instant Payments
AI-powered risk scoring analyzes payment urgency, beneficiary history, and contextual fraud indicators to Authorized Push Payment fraud in real time.