Hot topic Q&A – tackling card fraud in an era of new technology

Reports from around the world are showing a rise in card fraud. Fueled by technological advances and daring social engineering tactics, the fraudsters could easily get the upper hand. But it doesn't have to be this way. FICO fraud prevention expert Neil Mason outlines the issues and strategies that matter.

Neil Mason is a senior fraud consulting director in FICO's global domain presales team and has over 22 years' experience working in the fraud domain across a wide range of portfolios and channels. He specializes in supporting financial institutions in the optimization of their operational processes, strategies, and analytics as well as the implementation of fraud detection tools such as FICO® Falcon® Fraud Manager and fraud solutions on FICO® Platform.

Card fraud by the numbers

$49B

Projected global card-not-present (CNP) fraud loses over the next 10 years

Source

$33.8B

Worldwide payment card losses in 2023

Source

$404B

Worldwide payment card losses over the next 10 years

Source

80%

Estimated percentage of cards in circulation that are compromised

Source

Q1. Social engineering is a key strategy fraudsters use across many fraud types. How is it manifesting in card fraud, and what can issuers do about it?

Social engineering has become a dominant driver of debit and credit card fraud by targeting the most vulnerable element in the security chain: human behavior. Rather than directly attacking technical systems, fraudsters manipulate individuals into voluntarily surrendering sensitive data such as card numbers, CVVs, and one-time passcodes. In extreme cases we're even seeing fraudsters coerce victims to the point where they turn up at the victim's address and have them hand over their card and PIN number. Issuers increasingly refer to these threats driven by sophisticated and tailored deception techniques as "scams on cards."

Common tactics include phishing emails, impersonation calls, and fraudulent texts that closely mimic legitimate bank communications. In some cases, scammers guide victims step-by-step through processes designed to override the very security controls meant to protect them. These attacks often bypass traditional fraud detection systems, making them particularly challenging to identify with legacy tools.

What can be done?

Consumer education remains essential but must move beyond broad awareness campaigns that are easy to ignore. By leveraging FICO® Platform – Omni-Channel Engagement Capability for Fraud, issuers can proactively communicate with customers about high-risk transactions using the most appropriate channel—whether it's SMS, push notifications, or live calls. These timely, contextual alerts are far more effective at disrupting scams in progress.

Additionally, FICO has partnered with telecommunications providers to integrate telco data into scam detection. FICO® Customer Communications Service Scam Signal capability analyzes real-time network behavior to identify social engineering tactics, allowing institutions to intervene—by blocking payments or initiating customer outreach—before fraud is completed.

Q2. With people spending more time and money online, how are fraudsters taking advantage of their willingness to transact digitally?

The ease of setting up online storefronts and accepting card payments has accelerated legitimate digital entrepreneurship—but it's also created fertile ground for fraud. Scammers now create fake e-commerce operations that look highly credible, often using polished websites and targeted social media ads. Some even impersonate trusted brands to deceive consumers.

These schemes exploit the implicit trust consumers place in familiar logos and professional web design. Victims often realize they've been scammed only after failing to receive their purchases—by which time the fraudulent merchant has vanished or rebranded under a new identity.

What can be done?

Issuers and payment platforms must deploy advanced behavioral analytics to identify suspicious patterns in real time. AI models can detect anomalies in transaction flows and flag questionable merchants early in their lifecycle. Just as important are collaborative partnerships across the ecosystem—including social media platforms, domain registrars, and payment acquirers—to proactively remove fake merchants before widespread harm is done.

Q3. It feels like an arms race, with fraudsters rapidly adopting new technologies. How is this playing out?

Fraudsters are quick to exploit emerging technologies unconstrained by regulation or ethics. Key tactics include:

- Cyberattacks on businesses to steal customer data
- Carding bots and credential stuffing to automate stolen credential testing
- Remote access tools to hijack sessions
- SIM swaps to intercept one-time passcodes
- POS/ATM skimming for card cloning
- Use of generative AI to create convincing documents, video, and audio to scam consumers

This fast-paced evolution demands equally agile defenses. Financial institutions must invest in adaptive, real-time fraud detection systems powered by AI and machine learning. These models outperform static rules by continuously learning from fresh data and evolving fraud tactics.

There is growing interest in large language models (LLMs) and their ability to parse and analyze vast volumes of natural language data. However, general-purpose LLMs often lack domain precision. In contrast, focused models are trained exclusively on financial services data. These models deliver greater accuracy, interpretability, and speed in detecting financial fraud and recommending actions to mitigate threats.

Agility is critical. Fraud systems that require monthslong IT deployments to implement changes are no longer viable. Despite widespread investment in data science, a Gartner survey found that only 48% of AI projects reach production, often taking more than eight months to deploy. To stay ahead, institutions need solutions that support both rapid model development and operationalization without extensive overhead.

Q4. Financial institutions rely on data to fight fraud. What can they do to manage it better?

Effective fraud detection hinges on access to clean, integrated, and consistent data. Many institutions still operate in data silos, with card, mobile, and online activities captured in separate systems. This fragmentation prevents a unified view of customer behavior and weakens detection capabilities.

A 360-degree customer view—encompassing card usage, mobile app behavior, call center interactions, and more—enables AI models to detect fraud with greater precision. Quality training data enriched with well-labeled examples of fraud and legitimate activity is essential for building effective machine learning models.

But it's not just about internal data. External signals such as device intelligence, geo-location, and 3D Secure outcomes can significantly enhance fraud decisions. Adopting an API-first architecture allows issuers to flexibly integrate these third-party data sources, enabling faster and smarter fraud mitigation.

Q5. How does FICO help financial institutions prevent card fraud?

Much of my work involves helping FICO clients tackle card fraud and maximize the capabilities of FICO® Platform. It's exciting to witness how rapidly FICO is innovating in this field.

FICO's fraud solutions use real-time machine learning and contextual analytics to detect behavioral anomalies, even when fraud is masked through sophisticated social engineering. Our models continuously learn from evolving threats and are backed by over a hundred patents in fraud detection. FICO Platform enables institutions to build, test, and deploy their own AI and ML models quickly.

FICO also empowers institutions with omni-channel engagement, enabling real-time communication with customers during high-risk moments—via text, push, or phone—to interrupt scams in progress.

Lastly, our award-winning Scam Signal leverages telecom network intelligence to detect social engineering in action. By combining telco and financial signals, FICO helps stop scams before the card is ever used.

Learn more at

https://www.fico.com/en/solutions/card-fraud

FICO

Privacy Policy Terms and Conditions