FRAUD PREVENTION FRIDAY

Community Bankers of Michigan

Friday, November 14, 2025

Decoding and Defeating AI-Driven Financial Crime

Source: ICBA Fraud Task Force

The ICBA Fraud Task Force warns that synthetic media attacks, deepfakes, voice cloning, and AI-generated identities are no longer rare. Deepfake attempts have surged 2,137% since 2022, costing banks $200M in Q1 2025 alone. Criminals now bypass traditional security with tools that replicate voices in seconds and swap faces during live video calls.

Why it matters:

- Voice cloning defeats phone authentication with a 99% success rate.
- Video deepfakes undermine visual verification.
- Synthetic identities fuel account takeover and KYC fraud.

FinCEN now requires synthetic media detection under BSA/AML. Human-only detection fails up to 50% of the time, creating compliance exposure.

(*Click the heading link to read more.*)

Top News

Holiday Scams - Stay Alert

Each year, people worldwide are visited during the holidays and not just by family, friends, or Santa Claus. Rather, it's fraudsters and bad actors who take advantage of the seasonal spirit, and they can take the cheer out of your holiday.

Common Types of Scams

Find ways to share this information and educate your customers and all employees. Fraudsters use the latest technology to perpetrate a variety of fraud schemes headed to a community near you. The sophistication of these scams is continually increasing with advances in AI and other technologies. Be wary of solicitations on social media, search engines, text, and email, and keep an eye out for these schemes:

- **Charity Scams**. Scammers invent fake charities or spoof real ones to take advantage of those who want to help the needy during the holidays.
- **Fake Holiday E-Cards and Party Invitations**. Using a twist on the phishing playbook, fraudsters insert links in holiday e-cards and digital invitations that take you to bogus sites, then steal your credentials and/or distribute malware.
- **Fake Online Retail Stores**. Criminals send unsolicited emails containing links to fantastic deals at the website of a retailer you've never heard of or even ones that have been cloned.
- **Black Friday and Cyber Monday Scams**. The internet blows up with shopping ads for Black Friday and Cyber Monday. Malvertising schemes – i.e., fake ads for real stores – can more easily go undetected when people are expecting promotions.
- **Fraudulent Gift Cards**. Everyone loves the gift cards given – in person. Be on the lookout for fraudsters who claim you will receive a gift card by filling out a simple form, or sharing any personal details, which gradually lures you into providing sensitive information.

Security Maturity Improvement is Imperative as Cyberattack Risks Remain High

Source: Aunalytics

While advancing technology offers significant benefits, it has also made it easier for those who seek to gain an advantage by exploiting others. People intent on stealing your data or holding it to a hefty ransom are hidden in the digital web of interconnections, making the information age a double-edged sword.

An attack can be devastating for any business and impact it for many years to come. Today's organizations need digital sentries and multiple lines of defense against cybercrime.

According to a report released by Ponemon and IBM, 83 percent of organizations studied have experienced more than one data breach, and just 17% said this was their first data breach. Around 70% of successful cyberattacks exploited known vulnerabilities with available patches or known remediation steps. Identifying and resolving vulnerabilities is critical since a successful exploit can lead to a full-scale system breach.

Vulnerability management ensures that organizations have visibility around the latest known threats, preventing attacks before they occur. However, managing scanning or patching can be a challenge for smaller teams due to the ongoing cyclical management required. Setting up and coordinating manual ongoing patching across an organization can be extremely cumbersome, taking days to organize, schedule, and execute.

(*Click the heading link to read more.*)

Navigating the Rising Threats to ATM Security

Source: UFS

ATM crimes are not only a monetary threat to financial institutions but also a reputational one, demanding continuous innovation in ATM security both physically and cybernetically.

Evolution of ATM Threats

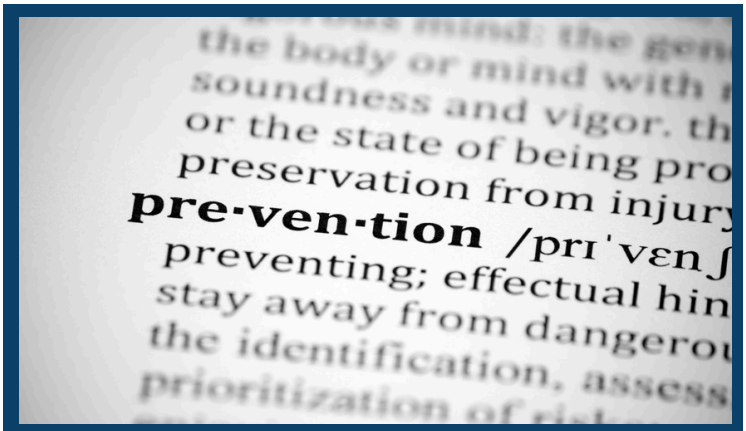
The journey of ATM security challenges can be traced back to the initial invention and networking efforts by Lloyd Bank in the late 1960s and early 1970s. Over the decades, modes of attack have transformed from physical — components stolen from ATMs or ATMs stolen from a location — to more aggressive and technologically advanced techniques such as skimming, jackpotting, malware, and card trapping. The evolution of these threats comes with a significant increase in ATM fraud cases. By the 2020s, rising incidents of ATM thefts set new records, with over 24,000 incidents reported annually.

Proactive Measures to Enhance ATM Security

Financial institutions must adopt a multifaceted approach to safeguard their ATMs. A comprehensive security strategy should include:

1. Recognize and Assess Threats: Regularly review your ATM fleet to identify vulnerabilities. Implement daily, weekly, and monthly audit procedures to inspect for tampering and suspicious skimmer devices.
2. Plan Your Security Requirements: Secure ATMs with unique institutional locks, add alarm contacts, and implement rigorous user access controls. Establish a robust password policy and ensure BIOS access is password protected.

(Click the heading link to read more.)



The Future of Fraud Prevention Is Orchestration, Not Detection

Source: Medium, Matan Naor

Fraud keeps winning, not because our tools are weak, but because our systems are.

For the past decade, financial institutions have been locked in an arms race of detection: new models, new vendors, new data feeds. Each one promised a step-change in accuracy, only for fraud losses to rise again as reported earlier this year by the FBI and by UK Finance. What if the problem isn't accuracy at all? What if it's architecture?

Modern fraud doesn't exploit flaws in individual systems. It exploits the gaps between them, the seams where data isn't shared, the delays between signals, the mismatched contexts between identity, payments, and customer experience.

Detection tools are doing their job. What's missing is orchestration, the ability to make the right decision across time, signals, and intent.

The Wrong Mental Model

Most organizations still treat fraud as a series of events: a login, a payment, a transfer. Each with an approve/decline/intervene decision.

But fraud doesn't unfold as events. It unfolds as journeys. Attackers don't break systems; they navigate them, exploiting how those systems interact.

That difference in mental model, event versus journey, isn't just semantic. It defines how companies structure teams, procure tools, and design controls. When you see fraud as a set of events, you create:

- Silos between fraud, identity, product, and customer experience teams.

(Click the heading link to read more.)