FRAUD PREVENTION FRIDAY

CBM™
Community Bankers of Michigan

Friday, March 20, 2026

With AI's Help, Fraudsters Are Targeting Smaller Banks

Source: U.S. News & World Report

Fraudsters impersonating banks were calling up customers, trying to convince them to reveal enough personal information to allow the criminals to hack into deposit accounts. On the surface, this was not unusual at all. Banks and consumers are regularly fighting off these types of schemes, and they are the kind of scam that Rivner sees daily as the CEO and co-founder of Refine Intelligence, which makes software that helps banks prevent fraud.

But this one stood out, both in its size and its strategy. Rivner says that by the end of the day, the banks he was tracking experienced a 1,700% spike in attacks. And instead of pretending to be representatives of the largest U.S. institutions, he says scammers were taking aim at smaller lenders. Half of the banks targeted, he says, had less than $3 billion in total assets.

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

Top News

How to Identify a Phishing Website

Source: knowbe4

Our increasing dependence on the internet and, specifically, email for business and personal communication has produced the perfect environment for cybercriminals to launch phishing attacks.

As organization's technical controls have advanced, cybercriminals have evolved their attacks, making them more difficult for traditional email security solutions that use signature-based detection (such as Microsoft and secure email gateways (SEGs) to detect. These attacks are also more difficult for people to spot as well. In results published from a phishing simulation, 53% of employees opened phishing emails and 23% input data into a form. Only 7% of employees reported the simulation to the Security team.

These numbers are concerning when you consider how costly data breaches can be for businesses. IBM estimates that the average cost reached $4.4m in 2025.

A phishing website is a website used by cybercriminals for malicious purposes, like credential theft or financial fraud. People frequently visit phishing websites having clicked on a phishing link in a malicious email. Phishing websites can be created using spoofed or lookalike domains or they can be built as part of a compromised legitimate website (this is a social engineering technique known as water-holing).

Cybercriminals can use phishing websites in multiple different ways. For example, the target might be presented with a log-in screen to enter their credentials, which are then scraped by the cybercriminal for use in account takeover attacks; or they might be prompted to enter payment details to confirm an order or pay for an item that will never arrive; or they might even automatically download malicious files or do so via a prompt on the webpage.

(Click the heading link to read more.)

Top Features to Look For in a Modern Fraud/BSA Platform

Source: Jack Henry

In today's fast-paced digital world, community banks are often caught between the dual pressures of ever-increasing digital transaction volume and sophisticated financial criminals who are constantly evolving their tactics.

Fraudsters are exploiting older, siloed systems, putting both your institution's assets and reputation at risk – especially in the era of instant payments.

For institutions with finite resources, merely trying to keep pace with these threats is no longer a sustainable strategy. To effectively protect your accountholders and communities, you need a single, unified, and intelligent defense system. Choosing the right fraud and BSA/AML transaction monitoring platform is the single most critical investment you can make.

But what exactly should you be looking for? Here are the top must-have features and functionalities to prioritize when choosing a modern platform:

- Unified Fraud and BSA/AML Monitoring (Holistic View) Fraud and money laundering often overlap, using the same accounts and methods. Why it matters: One unified platform provides a "single pane of glass" for analysts and investigators, merging all fraud-related activities (ACH, wires, faster payments, etc.) with BSA/AML monitoring. Eliminating these data silos helps ensure a comprehensive view of the accountholder's full risk profile, which is critical for catching complex, cross-channel fraud.

(Click the heading link to read more.)

Rising SMB Cyber Risk: Key Trends for Bankers

Source: PCBB BID Daily Newsletter

The number of data breaches in the US jumped 79% over the last five years to a record 3,322 data compromises in 2025, according to the Identity Theft Resource Center (ITRC). The financial services industry continued to have the highest number of breaches — 1,739 compromises, up from 733 in 2024, though down slightly from its peak in 2023.

While the number of breaches rose, the number of individual victim notices fell by 79%, from 1.36B in 2024 to 278.8MM in 2025 as hackers focus on fewer, but higher-value targets.

"The trajectory of data compromises in the US in the past five years shows the cybercrime and risk landscape has transitioned from mass identity theft — the accumulation of data — to pervasive identity fraud and scams, where stolen credentials are weaponized with precision," ITRC wrote.

Phishing, smishing, and business email compromises continued to be the top methods of breaches, while ransomware attacks dropped. Last year, physical card skimming made a comeback.

According to an accompanying ITRC report, SMBs are under near-constant cyberattack. Because of the uptick in incidents and the associated cost, many SMB cyber victims are now passing cyber incident costs through to customers, creating both higher direct and indirect risk for CFIs that serve SMBs, especially those providing credit and treasury services to them. Key SMB findings relevant to CFIs:

- Among businesses with fewer than 500 employees, 81% had suffered a security or data breach in the past 12 months. Most of these businesses experienced multiple attacks, with threat actors deploying increasingly sophisticated methods.

(Click the heading link to read more.)

A Practical Guide for Customers After a Scam or Fraud

Source: US Crypto Cop

Fraud and scams can happen to anyone, and when they do, the experience is often overwhelming. Customers may feel uncertain, stressed, or unsure of what steps to take next. The actions taken in the first hours and days after discovering a scam are critical to limiting financial loss and preventing further harm.

The Checklist for Victims, developed by the US Crypto Cop, provides clear, step-by-step guidance to help individuals respond quickly and confidently after fraud, identity theft, or other scam-related incidents. It covers essential actions such as securing accounts, stopping contact with scammers, reviewing transactions, reporting the incident to financial institutions and authorities, and documenting all related activity. It also highlights longer-term steps like monitoring credit, protecting devices, and staying alert for follow-up scams.

Community banks are trusted partners during these moments. This checklist supports the guidance bankers provide by reinforcing best practices and offering a practical roadmap for recovery. It also reminds victims that they are not alone, encourages them to seek support, and warns them about fraudulent "recovery" services.

Bankers can share this resource as a handout, follow-up tool, or educational aid to help customers regain control and move forward with confidence.

(Click the heading link to read more.)