FRAUD PREVENTION FRIDAY

Community Bankers of Michigan

Friday, May 15, 2026

Federal Reserve Releases Account Takeover Fraud Mitigation Toolkit and Enhancements to Existing Toolkits

Source: The Federal Reserve FedPayments Improvement

Reports of financial scams and fraud are continuing to escalate in number and sophistication year over year. The use of modern technology and the increase in new, emerging tactics are helping criminals be more successful than ever in their attempts to steal funds from individuals and businesses. Even older, less complex methods of fraud and scams are becoming more believable and harder to identify due to current techniques.

To address these new advancements in payments fraud, the Federal Reserve released a fourth toolkit – the Account Takeover Fraud Mitigation Toolkit – which details what Account Takeover Fraud is and how it happens.

Additionally, substantial enhancements have been made to our Scams Mitigation Toolkit and Check Fraud Mitigation Toolkit including a robust selection of new downloadable resources, and three new interactive "Test Your Knowledge" assessments.

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

Top News

Revealed: How Fraud is Evolving

Source: ICBA Independent Banker

When discussing bank fraud, the old adage “There’s nothing new under the sun” is apt.

Take phishing, a scam in which an individual receives an email requesting they wire a sum to Nigeria, Southeast Asia or even to a fraudulent account at what’s seemingly one’s own bank. While these requests were once littered with telltale typos or wonky logos, they now look quite convincing. That’s because ChatGPT allows anyone to send out letter-perfect requests in seconds.

Community bankers recognize that fraud is a growing problem.

“We’re seeing multiple threat vectors, as well as increased threat velocity,” says Anthony J. Ranghelli, chief information officer at $950 million-asset Potomac Bank in Charles Town, West Virginia.

As the types of financial fraud morph and multiply, community bankers are fighting on several fronts.

“We worry about deepfakes, and rightfully so,” says Scott Anchin, senior vice president of strategic initiatives and policy for ICBA. “But we also need to worry about these age-old fraud mechanisms that continue to exist. And they exist not only in their traditional forms but in new ways that make it more challenging to manage.”

The pain inflicted through financial fraud is attracting attention. In a late 2025 survey by Alloy, a fifth of financial institutions said they incurred losses from fraud of over $5 million in the past 12 months. What’s more, two-thirds (67%) of fraud professionals reported fraud events are on the rise.

(Click the heading link to read more.)

Six Key Online Fraud Trends to Watch in 2026

Source: Veriff

Online crime is evolving at an alarming pace. This article explores global online fraud trends, the risks posed by emerging technologies, and the opportunities for businesses to strengthen their defenses.

As fraudsters become more sophisticated, businesses and consumers face increasingly complex threats. From impersonation fraud to emulator and injection attacks, the landscape of online fraud is constantly shifting. Drawing on insights from the 2026 Identity Fraud Report, we project the following online fraud trends to dominate in 2026 and provide actionable strategies to combat them.

1. Impersonation fraud: The dominant threat

Impersonation fraud accounted for over 85% of all fraud attacks in 2025, making it the most prevalent form of online fraud. This method involves using stolen or falsified identity information to pose as someone else, often with counterfeit documents.

Despite its dominance, impersonation fraud has grown significantly more sophisticated in 2025, with fraudsters increasingly leveraging AI-generated deepfakes, synthetic identities, and document manipulation techniques to bypass traditional verification methods. This evolution—from high-volume, low-sophistication attacks to targeted, technologically advanced schemes...

(Click the heading link to read more.)

Much Faster Phishing Attacks Target Your Senior Execs via Microsoft Teams

Source: KnowBe4

A phishing campaign is targeting senior executives with social engineering attacks conducted over Microsoft Teams, according to researchers at ReliaQuest. The researchers believe former associates of the Black Basta criminal gang are running this operation.

“Black Basta was a prolific Russia-linked ransomware-as-a-service (RaaS) group active from early 2022 until its internal chat logs were leaked in February 2025,” the researchers write. “This campaign, likely conducted by former affiliates, uses an automated, two-pronged social engineering attack: mass email bombing to overwhelm a target’s inbox followed by Microsoft Teams-based help desk impersonation to gain remote access. In some cases, attackers moved from initial chat engagement to executing malicious scripts in as little as 12 minutes.”

The attackers are targeting senior employees to obtain a high level of privilege within the organization as soon as they gain access.

“This campaign's most significant evolution is its focus on targeting senior leadership, a tactic designed to secure high-privilege access from the very start and eliminate the need for noisy, time-consuming post-compromise escalation,” Reliaquest says. “In March 2026, 77% of attacks targeted executives, managers, and directors, up from 59% during January and February 2026. That increase likely reflects a direct refinement to the attackers' automated targeting: During the earlier period, most of the non-senior users targeted held titles such as project manager, a role that superficially resembles management but carries far fewer privileges. The removal of such roles from targeting scripts appears to account for the jump, suggesting threat actors are likely actively iterating on their open-web reconnaissance automation to improve the quality of their target pool.”

(Click the heading link to read more.)

Financial Institution Fraud Mitigation: Trends, Challenges, and Opportunitites

Source: ProSight

As fraud schemes become more prevalent and sophisticated, aided and abetted by AI, fraud mitigation has become a top priority for banks.

What are the most effective anti-fraud tools and techniques for banks to employ, and how are they accounting for the complex threats presented by AI? These were among the key issues addressed during a recent ProSight webinar featuring a trio of fraud experts: Matt Meis, cyber fraud and data manager at Summit Credit Union; Ray Olsen, senior vice president and director of enterprise fraud management at Wintrust Financial Corporation; and moderator Bobbie Paul, managing director of fraud at Huron.

Financial institutions regularly must manage and mitigate a plethora of aggressive AI-driven scams, from identity theft, ransomware, and phishing to account takeovers and business email compromise (BEC) schemes. But exactly how much more susceptible are banks and their customers to scams as a result of AI-driven fraud that looks and/or sounds authentic?

The democratization of cybercrime for entry-level bad actors is perhaps the biggest impact generative AI has had in the online fraud space. “GenAI is lowering the fraud entry barrier for all of those ‘new criminals’ who are looking to scam people,” Meis said, noting that high-level threat actors have been using AI tools like machine learning to perpetrate fraud for years.

(Click the heading link to read more.)