FRAUD PREVENTION FRIDAY

Community Bankers of Michigan

Friday, January 23, 2026

The Growth of Elder Fraud and What It Means for Your Institution

Source: CSI

Elder financial fraud has surged at an alarming pace, growing more than fourfold since 2020. Older adults are now among the most relentlessly targeted groups, facing schemes that range from familiar impostor scams to highly sophisticated attacks driven by breached data, AI-generated deepfakes, and coordinated criminal networks.

As this threat accelerates, community banks and credit unions are being pushed to the front lines. Customers now expect their institutions to detect and halt suspicious activity before it causes harm, even as financial responsibility increasingly falls on the very institutions working to protect them.

With 1 in 6 Americans now over the age of 65, scammers have a growing pool of high-value, financially vulnerable targets who have accumulated savings or retirement income.

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

Top News

The Fundamentals of Cyber Hygiene for Financial Institutions

Source: Conference of State Bank Supervisors

For bank and nonbank financial institutions, the modern threat environment presents an ever-expanding horizon of significant adversaries and attack methods – all aimed at crippling operations, extorting money from the institution, or stealing customers' sensitive personal information. In addition, the expanding world of artificial intelligence (AI), while introducing exciting new possibilities for institution efficiencies, also introduces new attack vectors and even AI-enhanced malware attacks for threat actors.

The Guide highlights the following critical threats against bank and nonbank financial institutions:

- Ransomware
- Geopolitical and hacktivist threats
- Social engineering and phishing
- Third-party risks
- Denial-of-service attacks (DoS/DDoS)
- Corporate account takeover (CATO)

The unavoidable truth is that today's cyber threats evolve at such speed that constant attention is needed to protect the institution and its customers from potentially devastating consequences. Ensuring that your institution has a program of strong, fundamental cyber hygiene practices in place today can significantly increase security protections against these (and other) threats and make your institution a less attractive target for cyber criminals.

Cyber Hygiene Fundamentals: A Guide to Securing Your Financial Institution Against Cyber Threats contains a catalog of fact sheets designed to provide a fundamental overview of how each of these controls and practices are critical to protecting institutions against existing and emerging cyber threats.

(Click the heading link to read more.)

Black Cat Hacker Group Uses Fake Notepad++ Websites to Distribute Malware and Steal Data

Source: gbhackers

A sophisticated cyberattack campaign orchestrated by the notorious "Black Cat" criminal gang has been uncovered by CNCERT and Microstep Online, revealing a coordinated effort to compromise internet users through weaponized fake Notepad++ download websites.

The operation exploits search engine optimization techniques to deceive unsuspecting users into installing malware-laden software packages that deploy backdoor trojans designed to exfiltrate sensitive data.

When users search for "Notepad++" on major search engines, a meticulously crafted phishing website appears as the second-ranked result, closely mimicking legitimate download portals.

This strategic placement exploits user trust in search engine rankings, significantly increasing the likelihood of successful compromise.

The phishing infrastructure demonstrates sophisticated social engineering, featuring realistic website designs complete with tutorial articles and multiple download options to enhance credibility.

Rather than directly linking to malicious payloads, the attackers employ a multi-stage redirection process that routes victims through authentic-looking download pages styled to resemble GitHub's interface, systematically lowering user suspicion before delivering the infected installer.

(Click the heading link to read more.)

Can You Spot a Fake Loan Text Scam?

Source: Federal Trade Commission Consumer Advice

You get a text message, supposedly following up on a $10,000 loan application. Only, you never applied for a loan. Is this pure luck or a scam? Before you use the callback number in the message to find out, or even reply "NO" to cancel the application, learn to spot a fake loan text scam.

Scammers use unexpected text messages to catch you off guard. Maybe the text says you're preapproved for a large loan amount (not true). Or the company says it needs your Social Security or bank account number to finish the "application" (also not true!). Scammers hope that, if it seems like the process is already in motion, you'll reply now and think later. They might say something like "This is the last step" or "Just reply YES to confirm you still want to claim the loan." But none of that's true, either. It's just a phishing scam. If you respond, you might end up giving a scammer exactly what they want — your personal information, which could lead to identity theft.

If you get a text about a loan you didn't apply for, here's how to handle it:

- Don't reply or click links. It could lead to a scam. Delete the text.
- Talk to someone you trust. Taking the time to talk about it with someone you trust could help you spot the scam.
- Delete unwanted texts using your phone's "report junk" option or forward them to 7726 (SPAM). Then report it to the FTC at ReportFraud.ftc.gov.

If you think a scammer already has your personal information, go to IdentityTheft.gov for specific steps to take based on the information you may have lost.

(Click the heading link to read more.)

Fraud and AML in Banking

Source: Banking Dive

If you get consumer-fraud experts in a room together, you'll generate a lot of talk.

That's what we found during Banking Dive's Fighting Payments Fraud event last February.

The problem is, financial institutions aren't talking to each other – either out of caution over perceived legal barriers, or out of stubborn competitive pride, some panelists said.

Victims, too, are undercommunicating, according to the Federal Trade Commission. Losses from fraud topped $10 billion nationwide in 2023, according to data from the agency. But that figure could be as high as $158 billion, the FTC noted in a follow-up report. Some experts blame shame for the gap.

The space surrounding fraud is far from silent, though. Payments firms offered potential fraud solutions to regulators on the issue. And one regulator suggested using artificial intelligence to fight deepfakes.

Talk can breed brand loyalty, too, one study found. Banks have 41% better customer retention when they track down fraudsters than when cases go without blame, professors at Notre Dame and Carnegie Mellon universities reported.

In this collection, we'll share what we've learned about consumer fraud in 2025. But consumers aren't the only victims. We'll give you a sense of how TD is recovering from the highest-profile anti-money laundering case in years. And how JPMorgan Chase and Jefferies are managing their connections to firms suspected of fraud.

(Click the heading link to read more.)