FRAUD PREVENTION FRIDAY

Community Bankers of Michigan

Friday, January 9, 2026

It's Beginning to Look a Lot Like Check Fraud

Source: LASCO

FRAUD! It's a word that no financial Institution wants to hear. But it's one that needs to be top-of-mind. Check fraud doesn't discriminate; it's relentless; it's enormously adaptable. It has been an unwanted visitor at the door, and as we approach the holidays, it can become a nightmare.

We know that fraud has always been there, but with the advancements in technology like AI, it is becoming harder for financial institutions to manage. The real problem is that fraudsters are getting smarter and more sophisticated.

Whether we're talking about BIN attacks, debit card fraud, ATM fraud, Phishing, Smishing, Vishing, wire & ACH fraud, or identity theft, some threats are becoming more difficult to mitigate.

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

Top News

Justice Department Announces Seizure of Stolen-Password Database Used in Bank Account Takeover Fraud

Source: Department of Justice Office of Public Affairs

The Justice Department recently announced the seizure of a web domain and a database used to further a scheme to target and defraud Americans through bank account takeover fraud. The domain, web3adspanels.org, was used by those involved in the scheme as a backend web panel to store and manipulate illegally harvested bank login credentials. This domain seizure comes approximately one month after the FBI issued a Public Service Announcement relating to Account Takeover Fraud via Impersonation of Financial Institution Support.

According to the affidavit filed in support of the domain seizure, the criminal group perpetrating the bank account takeover fraud delivered fraudulent advertisements through search engines, including Google and Bing. These fraudulent advertisements imitate the sponsored search engine advertisements used by legitimate banking entities. While the fraudulent advertisements appeared to direct users to legitimate bank websites, victims were redirected to fake bank websites controlled by the criminals. When victims entered their login credentials to access their bank accounts, the criminals harvested those credentials through a malicious software program embedded in the fake website. The criminals then used those bank credentials on the corresponding legitimate bank websites to access victims' bank accounts and drain their funds.

To date, the FBI has identified at least 19 victims throughout the United States, including two companies in the Northern District of Georgia, whose bank accounts have been compromised through this account takeover scheme, resulting in attempted losses of approximately $28 million dollars and actual losses of approximately $14.6 million dollars.

(Click the heading link to read more.)

Cyber, Fraud, and AI: Linked Risks, Multiple Entry Points

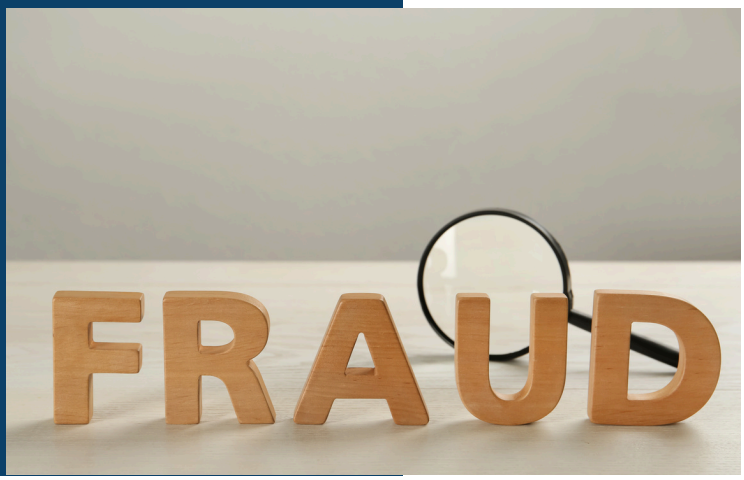
Source: ProSight

Technology and cyber risk now sit at the center of numerous banking challenges—and they're increasingly fueling fraud. In ProSight's 2026 CRO Outlook Survey, 74% of respondents ranked technology and cyber among their top five risks. CROs said the ongoing push toward digitalization and AI gives bad actors more ways in, while connecting new systems to old infrastructure creates integration weak spots. Geopolitical risk—named a top risk by 22% of respondents—adds another layer, as nation-states target critical infrastructure like financial services.

Fraud is increasingly AI-enabled. Fraud and financial crime ranked No. 2 on the list of top risks, named by 55% of respondents, and survey comments stressed the interplay with cyber, AI, and geopolitics. A large bank CRO warned: "If you combine cyber, AI, and what will happen in the coin space, you will see a faster proliferation of fraud. The threat actors are going to be able to move more nimbly than the governance." Real-world attempts are getting harder to spot. The same CRO said a fraudster emailed a client while impersonating him—the message "read like an email I would send. It was near flawless." Nearly a third of respondents (32%) said the possibility that AI could be used to perpetrate fraud was a top AI-related risk.

Third-party risk is the fault line. Given the expanding attack surface, about a quarter of respondents identified operational resiliency as a top risk. One large-bank CRO called out third-party exposure specifically—both as a gateway for exploits and as a reason banks may need to sever connections quickly during an incident to contain spread.

(Click the heading link to read more.)



When Fraud Strikes, Customers Want Answers, Not Just Refunds

Source: PCBB BID Daily Newsletter

A new large-scale research study from the University of Notre Dame and Carnegie Mellon University — reviewing data from over 420K customer fraud cases provided by a major US bank — reveals that the outcome of a fraud investigation is crucial for customer retention. Customers who experience fraud in which the institution could not identify a perpetrator are 41% more likely to leave than those who never faced fraud.

In contrast, when a financial institution is able to attribute blame and demonstrate to the customer that the fraudster was identified, not only does retention recover, but loyalty is reinforced. Even fewer customers who experienced fraud switch institutions in those instances than among those who have never suffered fraud.

The study provides more granular insight into how financial fraud affects customer loyalty. Another survey in 2024 found that 75% of consumers globally would switch banks if they discovered that their bank's fraud protection measures were insufficient.

The results of the latest study are surprising not only to banks but to the researchers from the University of Notre Dame and Carnegie Mellon University. Vamsi Kanuri, an associate professor at the University of Notre Dame who served as a researcher on the study, told U.S. News magazine: "We never thought in our wildest dreams that we'd actually find this in our study."

The findings challenge the assumption that uncovering fraud and refunding losses is sufficient. This unexpected prioritizing of identifying the entity behind the fraud underscores how perceptions of competence hinge on visible investigative follow-through. The lesson is that a shrug won't do when a defrauded customer asks about the origin of the fraud.

(Click the heading link to read more.)

Spot the Scams When Fixing Your Credit

Source: Federal Trade Commission

Please share this article with your customers who may be considering credit repair services. It could save them money and protect them from fraud.

If there's information on your credit report that's correct but not so great, it can make it harder to get credit with good terms. But there are things you can do yourself for free to help fix your credit. Credit repair companies also charge to do the same things. Before you consider paying, though, know the rules these companies have to follow — rules dishonest companies and scammers often break.

Before they do any work for you, credit repair companies have to write up a detailed contract that explains your legal rights (like your three-day right to cancel without any charge) and the total cost of their services. It's illegal for credit repair companies to lie about what they can do for you, charge you before they help you, or ask you to lie on credit applications. Credit repair companies also can't legally remove negative information from your credit report that's correct and up to date.

Here are some ways to help fix your credit:

- Fix mistakes in your credit reports. Get your free credit report from AnnualCreditReport.com. If you see a mistake, write to the credit bureau and the business that reported the information. For more information, read Disputing Errors on Your Credit Reports.
- Pay your bills on time, pay off debt, and don't take on new debt. It takes time to improve your credit. If there's accurate negative information in your credit report, credit repair companies can't remove it for you legally. It'll go away with time.
- Find real help. Your local community bank, university, or military personnel financial manager might be able to recommend a non-profit credit counseling program that can help.

(Click the heading link to read more.)