FRAUD PREVENTION FRIDAY

Community Bankers of Michigan

Friday, July 10, 2026

ICBA Releases Guide on Partnering with Law Enforcement to Combat Fraud

Source: ICBA

Community banks can play an important role in fraud prevention as front-line observers. By leveraging their close relationships with the local customer base, community banks are often well positioned to help in the fight against fraud. With appropriate staff and training, community banks may be among the first to notice suspicious transactions, altered checks, and other signs of fraud. Early awareness can help limit further harm.

Many community banks share information with their customers about fraud risks and prevention strategies, including secure banking practices such as using strong passwords, recognizing phishing attempts, staying informed about current scams in the region, and safely handling checks. When fraud occurs, community banks may assist customers in addressing the situation and securing their accounts, and provide guidance to help them feel comfortable again.

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

Top News

SIM Swap Fraud and Phone-Number Hijacking Explained

Source: SHAZAM

Your phone number used to be just a way to make and receive calls. Today, it acts as a digital ID tied to your bank account, email, social media and work logins. That shift is why SIM swap fraud has moved from a niche scam to a fast-growing risk.

SIM swap fraud happens when criminals trick a mobile carrier into transferring a victim's phone number to a SIM or eSIM they control. Once that happens, text-based login codes and password resets go straight to the attacker, enabling rapid account takeovers without hacking a device. Law enforcement reports show the tactic is increasingly used as the first step in larger fraud schemes, especially those involving financial and cryptocurrency accounts.

The trend is accelerating because stolen personal data is widely available, customer support processes still rely on human judgment, and many organizations continue to depend on text messages for account security.

According to the FBI's most recent Internet Crime Report, cyber-enabled fraud reached record losses in 2025, with identity-based attacks — including phone-number takeovers — playing a central role in larger financial scams. As criminals look for high-impact fraud methods, SIM swap fraud has become a reliable entry point.

How SIM swapping works

Most people secure important accounts with a password plus a second step, often a text message code. In a SIM swap attack, the criminal doesn't need to defeat your phone. Instead, they target the carrier process so your number is redirected to their device. From there, password-reset links and texted authentication codes can land in the attacker's inbox.

(Click the heading link to read more.)

Don't Send Checks Through the Mail. Just Don't

Source: New York Times

A practice that was common not so long ago has become increasingly risky — sending checks in the mail. But if you must send money this way, scour your account statements promptly.

Skipping that advice can leave you vulnerable to check fraud, and may also make it more difficult to recover the money if you lose it.

Joan K. Atchinson, 63, a retiree who lives in Washington, D.C., is dealing with that right now.

Ms. Atchinson said in a phone interview that she was trying to recover several thousand dollars stolen when someone intercepted a check she mailed last year. The check was altered to be payable to someone else before it was cashed. After months of trying, she said, she still has not recovered payment from either of the two banks involved — Charles Schwab, where she has an account that she used to write the check, and Chase, where the falsified check was cashed. "I've kind of lost hope."

How does this kind of check fraud work?

Checks sent through the Postal Service have become targets for criminals in recent years. While fewer people write checks, the checks haven't disappeared. Two-thirds of adults say they rarely or never use paper checks, but more than a fifth either have experienced check fraud or know someone who has, according to a poll in 2025 by the Independent Community Bankers of America, a trade group.

(Click the heading link to read more.)

How to Avoid Typosquatting Scams

Source: SHAZAM

Online banking, payment apps and investment tools make everyday financial tasks easier than ever. But the same convenience that helps accountholders also gives scammers new ways to take advantage of simple mistakes — like one mistyped letter in a web address. Learning how to avoid typosquatting scams can help accountholders protect their financial information online.

What is typosquatting?

Typosquatting, or URL hijacking, happens when cybercriminals register website addresses that look almost identical to trusted sites. They rely on users making small typing errors or clicking too quickly. These look-alike and fake banking websites can be convincing, and once someone lands on one, they may be prompted to enter login credentials or other sensitive financial information.

The good news is that a few simple habits can make a big difference in protecting accountholders and overall online banking security.

How do typosquatting scams work?

Typosquatting scams succeed because they take advantage of normal human behavior. We're busy. We move quickly. And sometimes, one extra letter, a missing character or the wrong domain ending — such as ".org" instead of ".com" — is all it takes to send someone to the wrong site. Scammers don't always need to break into systems. Sometimes, they just need someone to be in a hurry.

How can financial institutions help accountholders stay safer online?

(Click the heading link to read more.)

A Layered Defense Against AI-Driven Fraud

Source: ProSight

AI has made fraud faster, more polished, and easier to scale. It is also giving banks and credit unions new ways to detect altered documents, stop spoofed calls, monitor transactions, and prioritize suspicious activity.

In a reported feature for the June 2026 ProSight Executive Report, Jason Bartolacci, director of the ProSight Fraud Alert Network, examines both sides of that contest, which is also a key theme in the just-launched ProSight State of Fraud Prevention Survey. Using Logix Federal Credit Union as the primary operational case study, he shows how one institution is responding to AI-enabled account takeovers, synthetic identities, voice cloning, and other rapidly evolving threats.

Several practical lessons emerge from Logix's experience:

Prepare for attacks aimed directly at customers. The fraud landscape has shifted as criminals increasingly target customers rather than trying to break into accounts through bank contact centers. AI-generated phishing, cloned voices, and personalized messages can make those approaches appear legitimate while allowing criminals to launch them rapidly and at scale. Logix sees account takeover attempts through fake calls and texts hundreds of times a day.

Verify documents before fraud becomes a loss. The credit union uses an AI-powered document authenticity tool to review bank statements,...

(Click the heading link to read more.)