FRAUD PREVENTION FRIDAY

Community Bankers of Michigan

Friday, July 24, 2026

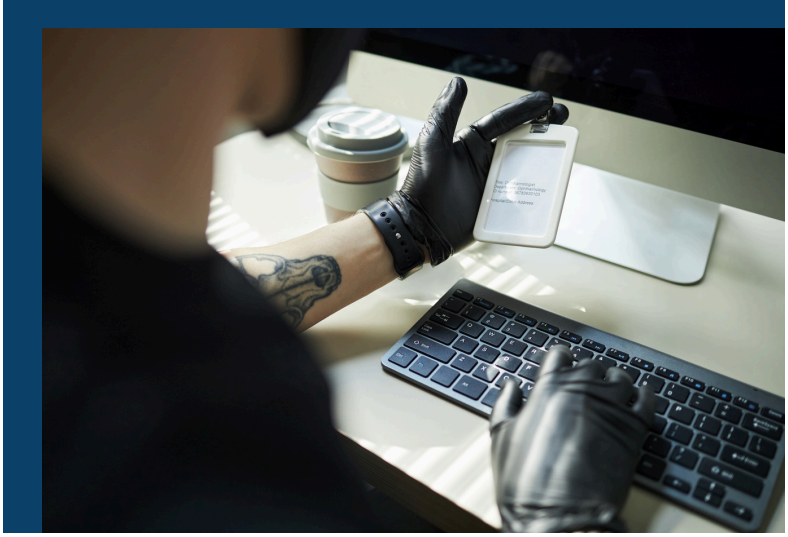
FinCEN Update: Combating Fraud and Modernizing Anti-Money Laundering Oversight

Source: Financial Crimes Enforcement Network

Andrea Gacki, Director of FinCEN, testified on July 21, 2026, about efforts to combat fraud and modernize anti-money laundering regulations. She highlighted FinCEN's Rapid Response Program, which has helped recover nearly $2 billion in stolen funds for U.S. victims since 2015, and actions against the Huione Group for laundering billions in illicit proceeds. FinCEN is also advancing a whistleblower program to encourage reporting of financial crimes. To address evolving threats, FinCEN is updating the Bank Secrecy Act framework, including reforms to Suspicious Activity Report requirements and AML/CFT programs to emphasize effectiveness and reduce unnecessary compliance burdens. The agency has also proposed rules for stablecoin issuers under the GENIUS Act while seeking resources to strengthen oversight and fraud prevention.

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

Top News



Scammers Are Using FaceTime to Steal Bank Account Passwords

Source: Veritas Security Advisors and CBS News

A growing scam relies on Apple's popular FaceTime video calling app, with fraudsters using the service to impersonate bank representatives and drain consumers' bank accounts.

According to CBS News national consumer correspondent Ash-Har Quraishi, the scammers convince consumers they need to provide information to verify their bank accounts.

Victims first receive a text message about account activity related to their bank or credit card, and are asked to call a phone number included in the text. Other times, they receive a direct call from the scammer, who says they require "additional verification."

That's when the fraudster switches from an audio-only call to FaceTime. Victims are tricked into sharing their computer screens with the scammers while they log into their online banking accounts.

"The scammer watches in real-time while victims expose passwords, account numbers and even one-time security codes," Quraishi said.

Apple says scammers are exploiting FaceTime because consumers generally trust the app and view it as a secure platform.

But the tech giant urges consumers who believe they're receiving a suspicious FaceTime call from someone posing as a bank representative to take a screenshot of the call.

Tap the "info" button next to the call, hit "take live photo," and send the image to reportfacetimefraud@apple.com.

(Click the heading link to read more.)

How New Nacha Rules Help Fight ACH Fraud

Source: ICBA Independent Banker

Nacha, the organization that governs the nation's ACH network, has implemented two new rules for financial institutions intended to reduce the incidence of successful scam attempts and improve the recovery of funds after fraud has occurred.

The first rule introduces new risk-based practices, particularly for institutions receiving and sending funds. The second rule standardizes descriptions for different types of payments to enable institutions to better tailor their fraud mitigation.

Read on for what community banks need to know to navigate these new Nacha rules and tools that could make it easier.

Nacha Risk Management Compliance for ODFIs and RDFIs

The first rule, on risk management, requires that both originating depository financial institutions (ODFIs) and receiving depository financial institutions (RDFIs) implement risk-based processes to identify ACH entries initiated due to fraudulent scams.

Previously, Nacha only required ODFIs to use a fraudulent transaction detection system to screen online and mobile (WEB) debits and when using micro-entries. Now, RDFIs should be evaluating behavior signals for fraud risk, such as incoming transactions, as well as account profile information and historic activity on the receivers' accounts.

(Click the heading link to read more.)

ClickFix Social Engineering is Now the Leading Malware Delivery Method

Source: KnowBe4

The ClickFix social engineering technique is now the top malware delivery method, according to a new report from ReliaQuest. These attacks trick users into copying a malicious command, then pasting it into a terminal and running it on their computers.

"ClickFix remained the dominant delivery method this period and, for the first time, we observed it expand to macOS, delivering infostealers onto a platform many organizations still monitor less closely than Windows," the researchers write. "This means ClickFix can no longer be handled as a special case. Training, detection, and triage for it should run continuously on both Windows and macOS."

ReliaQuest notes that AI tools are enabling threat actors to scale social engineering attacks with very little added effort.

"Adversaries leaned on two strategies: social engineering at scale and attacks on unpatched, internet-facing infrastructure," the researchers write. "The leading technique 'ClickFix' drove the first, shifting delivery from compromised websites to emailed links, while 'Qilin,' the period's most active ransomware operator, continued exploiting unpatched edge devices for mass extortion. What's more, AI is making social engineering faster, cheaper, and more convincing, accelerating familiar techniques rather than creating new ones."

Organizations should ensure that their security awareness programs train employees to recognize ClickFix tactics.

(Click the heading link to read more.)

Passkeys: Cutting Fraud, Friction, and Support Cost

Source: PCBB BID Daily Newsletter

Most people can only juggle about three to five things in their working memory at once, so it's no surprise that managing dozens of complex passwords has always been a losing battle, one that set the stage for today's shift toward passkeys. Faced with that cognitive limit, users have long defaulted to reusing simple passwords or writing them down, trading security for convenience. Over time, that human workaround created exactly the kind of vulnerability hackers rely on, turning password management into a persistent weak point in digital security.

An arms race between hackers and legitimate website users has been spiraling ever since users have been able to transact with websites. Users had passwords to protect them, but it was tough to think up secure passwords and remember them all, so many people used recycled one or two passwords across multiple websites. That made it easier for hackers to guess the passwords.

Password managers sprang up as a place to store multiple complex passcodes, but again, that left access to every account locked behind just one password. Two-factor authentication is more secure, but hackers can intercept codes, and many users didn't appreciate having to jump through another hoop on their way to website access. Passkeys take the place of passwords and two-factor authentication.

Passkeys: How They Work and Where Adoption Stands

(Click the heading link to read more.)