FRAUD PREVENTION FRIDAY

Community Bankers of Michigan

Friday, May 29, 2026

Building Momentum: Progress on Reg CC, the UCC, and the Fight Against Check Fraud

Source: ICBA

A couple years ago, I wrote that check fraud was emerging as a leading concern for community banks, that combating it would require shared responsibility across the financial ecosystem, and that ICBA was just kicking off a community bank check fraud task force to help lead the way.

Real progress on check fraud has never come from a single breakthrough. It comes from sustained advocacy, patient relationship building, and the slow accumulation of small wins. Community banks are in the middle of that arc, and the work is paying off.

Where we've gotten traction

A few headline-grabbing victories stand out. Federal policymakers are aligned on the urgency of check fraud in a way they were not before.

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

Top News

Attackers Continue to Pose as Help Desks in Social Engineering Attacks

Source: ICBA Independent Banker

Researchers at Google's Threat Intelligence Group (GTIG) are tracking a new threat actor that's impersonating help desks to trick users into installing malware. The threat actor, which GTIG tracks as "UNC6692," begins by sending a large volume of spam emails to the victim, then initiates contact via Microsoft Teams to ostensibly help the user block the spam.

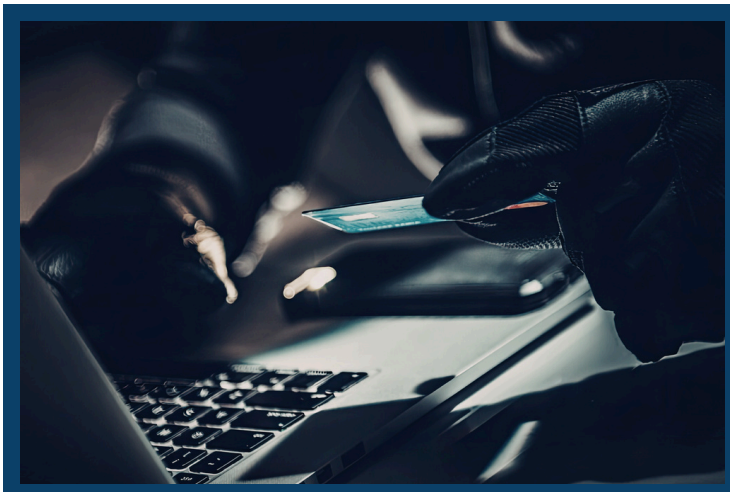
"As with many other intrusions in recent years, UNC6692 relied heavily on impersonating IT helpdesk employees, convincing their victim to accept a Microsoft Teams chat invitation from an account outside their organization," GTIG says. "The UNC6692 campaign demonstrates an interesting evolution in tactics, particularly the use of social engineering, custom malware, and a malicious browser extension, playing on the victim's inherent trust in several different enterprise software providers."

After the attackers make contact with a victim on Teams, they send a link to a phishing page that poses as a "Mailbox Repair Utility." This page is designed to harvest the user's credentials.

"The harvesting script…employs a 'double-entry' psychological trick. "It is programmed to reject the first and second password attempts as incorrect. This serves two functions: it reinforces the user's belief that the system is legitimate and performs real-time validation, and it ensures that the attacker captures the password twice, significantly reducing the risk of a typo in the stolen data."

The phishing page then installs several strains of custom malware to establish a foothold on the user's system.

(Click the heading link to read more.)



Why Faster Payments Are Raising the Compliance Stakes

Source: ProSight

Faster payments and digital transactions are often framed as a customer experience story. But the just-released 2026 ProSight Compliance Outlook Survey suggests they are also becoming a compliance story—especially as fraud adapts to speed, scale, and AI.

The issue is no longer just that digital payments are growing. It is that as funds move faster and criminals get better tools, compliance teams are being pulled deeper into fraud prevention, electronic transaction monitoring, and cross-functional coordination.

A few practical points stand out:

Payment speed is changing the fraud equation. In the survey, 58% of respondents said payment systems such as ACH, RTP, and Fedwire are likely to require more time, management attention, and resources over the next three years. Another 54% said compliance spending tied to electronic transactions increased by 5% or more from 2025 to 2026. The report notes why: electronic transactions are "prime targets for fraud, especially as faster payments make recovering funds exceedingly difficult."

Compliance can't treat fraud as someone else's problem. The survey connects payment innovation directly to financial crime risk. As one senior line of business executive at a community bank put it, "Fraudsters shift constantly and crime evolves as quickly as new financial products become available."

(Click the heading link to read more.)

AI-Fueled Scams Drive Fraud: Visa

Source: PaymentsDive

Although payment threats are showing signs of slowing, Visa cautioned that fraudsters are exploiting human vulnerabilities and AI to carry out their attacks.

In its report, Visa noted that cybercriminals are using AI to automate their attacks, but the card network also said it is using the technology to block attacks sooner and reduce potential losses.

One key lesson: cybersecurity strategies that involve slow-moving patterns and manual review are no match for threat actors using machines, the report said.

“Criminals are increasingly targeting people rather than technology, using deception, urgency and AI-enabled tools to exploit trust,” Fabara said in the press release.

To address that shift toward people will require “continuous innovation at the network level and close collaboration across banks, merchants, policymakers and the broader payments ecosystem,” he said.

Global ransomware attacks jumped 26% from 2024 to 2025, but less than one quarter (23%) of victims paid ransoms to perpetrators, the report said. Many organizations are reluctant to pay ransoms “as victims have learned paying has little effect on whether their sensitive data is leaked to the public,” the release said.

Of the victimized organizations that paid ransoms, the size of payments plunged 66% between July and September 2025 compared to the prior three months, Visa said in the report. A Visa spokesperson declined to provide additional information about ransoms paid.

Along with Visa, other payments insiders have warned that AI is accelerating fraud.

In a report released in March, Nasdaq’s Verafin unit found that the money pilfered worldwide by online criminals...

(Click the heading link to read more.)

Small Banks, Big Targets: Rising Threats of Cybercrime for CFIs

Source: PCBB BID Daily Newsletter

There's no shortage of risks to consider when it comes to protecting your digital accounts and devices, and it's more important than ever to have all your bases covered. Cybercrime is increasing within the financial services industry, and vulnerable community financial institutions (CFIs) and their customers are now fraudsters’ favorite targets. Americans last year suffered nearly $21B in losses due to internet crime. For the financial services industry specifically, $275MM in losses were recorded, a 59% increase from 2024, according to the FBI’s 2025 Internet Crime Report.

The report, which recorded more than 800K complaints, underscores that the majority fall into “cyber-enabled crime” — schemes that originate online but result in real-world financial loss. Phishing and spoofing ranked as the most reported crime type, followed by extortion and personal data breaches, while business email compromise (BEC) and investment scams remained among the most financially damaging. In many cases, these crimes begin with a digital touchpoint and ultimately lead to fraudulent wire transfers or ACH payments.

CFIs are Increasingly Targets

CFIs and their customers are ideal targets because they don’t have the type of robust security resources that bigger banks do, like dedicated cybersecurity specialists and operations centers whose budgets often surpass a CFI’s budget across its entire operations. Bigger banks have also cultivated mature defenses with rapid response capabilities and aggressive legal teams.

(Click the heading link to read more.)