FRAUD PREVENTION FRIDAY

Independent Banks of South Carolina

Friday, July 11, 2025

New ICBA Polling Shows Public Support for Policy Efforts Targeting Check Fraud

Source: ICBA

Following federal banking regulators' recently issued request for information on potential agency actions to address check fraud and other forms of payments fraud, the Independent Community Bankers of America (ICBA) announced polling results showing Americans support policy efforts to take on the scourge of check fraud. According to ICBA polling conducted by Morning Consult in June:

- More than one-fifth of U.S. adults have or know someone who has experienced check fraud, even though two-thirds rarely or never use paper checks.
- 80% agree that policymakers should address the rise in check fraud.
- 73% agree that the Treasury Department should consider alternatives to issuing paper checks to help prevent fraud.

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

Top News

Processors Lean on AI to Fight Fraud

Source: Payments Dive

For payments processors fighting a rising flood of fraud, artificial intelligence is a key weapon, according to a trade group that represents such service providers.

The American Transaction Processors Coalition has urged Congress members and staff to avoid regulating AI in any way that would hamper payments companies' use of the evolving tool, said West Richards, the group's executive director. That's because payments companies will increasingly depend on AI to fight criminals who are tapping the technology for wrong-doing, he said.

The issue surfaced this week as Congress members debated the budget and spending reconciliation bill, including a provision that would have prohibited states from regulating AI for ten years. On Tuesday, that moratorium was stripped from the bill in a 99-1 Senate vote, preceding passage of the entire bill by that chamber. There is no federal regulation that is specific to artificial intelligence.

The ATPC, which represents card company American Express, payments firm Deluxe and processor Fiserv, among others, had no official position on the AI provision that was taken out of the bill, but allowing states to weigh in with AI regulation may not be what the coalition had in mind.

"The main thrust is, do not handicap us with AI, because we need AI to fight AI," Richards said in an interview last month, before the Senate vote. "These cyber-attacks and these fraud attacks, more and more are being AI-driven, so we need flexibility in utilizing AI to combat those threats."

(Click the heading link to read more.)

Uncover Your Cyber Vulnerabilities: Better Protection Starts With Penetration Testing and Vulnerability Assessments

Source: Rehmann

Your IT team is diligent. You've invested in robust firewalls, modern hardware, regular software updates, and even a backup server. But here's the critical question you must regularly ask yourself: "Is my data and IT systems safe enough from cyberattacks?" And just as importantly: "How do I know?" The reality is that our fast-paced digital world introduces new threats every day. Even with a strong defense, vulnerabilities can seep through unnoticed, leaving your organization exposed to potential risks. This is where vulnerability assessments and penetration testing prove invaluable. Vulnerability assessments and penetration testing are methods of identifying and mitigating cybersecurity risks. While they share a common goal — improving security against potential cyberattacks — they differ in approach.

- Vulnerability Assessments: Think of a vulnerability assessment like a would-be intruder walking around the exterior of your home in search of potential entry points. He'll rattle doorknobs, try to jimmy open your windows, and poke around to see if you have a dog or alarm system.

(Click the heading link to read more.)

Collaborating to Turn the Tide Against Fraud in the Financial Sector

Source: BAI

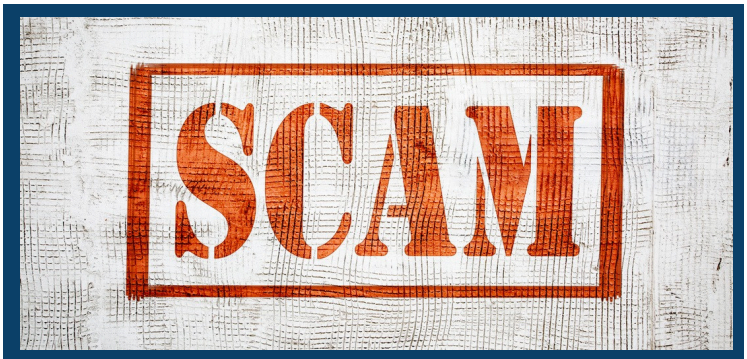
In an era where fraudsters grow more sophisticated by the day, collaboration has never been more critical. The CBM Risk Fraud Forum offers a vital opportunity for financial professionals across Michigan to unite, share insights, and strengthen their collective defenses. By participating in this forum, attendees tap into a powerful network of peers committed to safeguarding the financial ecosystem. As highlighted in BAI's recent article, cross-institutional collaboration is proving to be one of the most effective tools in turning the tide against fraud. Together, we can build a more resilient future—one conversation, one strategy, and one partnership at a time. Read the full article here.

Consumer trust and institutional stability is under attack. Why? In a simple word: Fraud.

Fraud is reshaping the global financial sector, introducing risks that extend beyond monetary losses. Sophisticated schemes such as authorized push payment (APP) scams, synthetic identity fraud and vast mule networks means that financial institutions need to advance digital fraud protections and fast.

One good thing that came out of the pandemic is that it forced companies and consumers to embrace an expedited digital evolution, but with the emergence of new, more convenient payment types comes more risk and complex threats.

(Click the heading link to read more.)



Help Customers Outsmart These Four Financial Scams

Source: PCBB's BID Daily Newsletter

Now that financial institutions have instituted more effective controls to combat fraud, criminals are increasingly taking the path of least resistance and targeting customers directly with scams. Here are four popular scam types impacting community financial institutions' (CFIs') customers, along with ways your institution can combat them.

1. Check fraud. Check fraud is rampant at the moment, causing headaches for CFIs, consumers, and businesses. These are a few of the most common ways scammers use checks to commit fraud:

- Creating fake checks or forging a signature and cashing an existing check
- "Washing" checks, by substituting the original information with new information
- "Kiting" checks by writing a higher amount than what's in the account, and depositing the check at another institution
- Sending a check to an unwitting victim, with fine print legally binding them to a contract, called "unsolicited check fraud"

How CFIs can help: "One of the strongest and most effective" tools to protect against check fraud is offering business customers positive pay automated monitoring with payee match, which double-checks whether names on checks match those already on file. "Our clients say it's a real game-changer and it provides peace of mind," says Sarena Barker, senior vice president and digital banking manager at the $1.6B-asset Plumas Bank in Quincy, California.

(Click the heading link to read more.)