FRAUD PREVENTION FRIDAY

Independent Banks of South Carolina

Friday, August 15, 2025

Can't Access the Links in the Fraud Prevention Friday Newsletter? Let Us Know!

We know how important it is to stay informed about the latest fraud trends, scam alerts, and prevention tools, which is why our Fraud Prevention Friday newsletter is packed with timely articles, downloadable resources, and trusted links. However, we also understand some banks' cybersecurity policies may restrict employees from clicking on external links within emails. If that's the case at your institution, we want to help. If your team is unable to access the links or attachments in the newsletter, please reach out to the IBSC team. We're happy to provide the same content in an alternative format, whether it's a PDF version of the newsletter with embedded articles, direct attachments, or another delivery method that works for your bank's policies. Our goal is to ensure every community banker has access to the critical information and tools included in the Fraud Prevention Friday newsletter, regardless of their firewall or filter settings. Please contact April Folger at afogler@myibsc.org so we can ensure you receive the full benefits of the newsletter. Together, we can keep your team and your customers better protected.

Top News

- Can't Access the Links in the Fraud Prevention Friday Newsletter? Let Us Know!
- Staying Ahead of the Scam: How Community Banks Can Continually Educate Staff and Customers on Fraud Prevention
- Banks Can Stop Synthetic Identity, Abuses by Moving as Fast as, Fraudsters
- On The Right Side of AI
- Protecting Small Business From Check Fraud: Why Positive Pay is a Must-Have Tool

How Community Banks Can Continually Educate Staff and Customers on Fraud Prevention

Source: Community Bankers of Michigan

Fraud is no longer a seasonal threat or a one-time training topic; it's a persistent, evolving challenge that requires constant attention and education. That's why our friends at CBM have developed a new guide for community banks "*Staying Ahead of the Scam: How Community Banks Can Continually Educate Staff and Customers on Fraud Prevention*."

This document is designed to help your bank build and sustain a culture of fraud awareness by offering practical ideas, curated resources, and ready-to-use tools to keep both employees and customers informed and vigilant.

Fraudsters are constantly shifting tactics, whether it's through phishing, text scams, social engineering, or check fraud, and both customers and frontline staff need regular updates to stay protected. Many banks want to do more to keep their communities informed, but aren't sure where to start or how to keep up.

That's where *Staying Ahead of the Scam* comes in. This document includes:

- Strategies for continuous staff training on fraud awareness.
- Tips for sharing timely fraud education with customers via newsletters, social media, and in-
- branch signage. Links to trusted resources and printable materials from the FDIC, FTC, and more.
- Tools to create your own branded fraud prevention hub on your website.
- Ideas for community outreach, including seminars and senior-targeted education sessions.

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

Banks Can Stop Synthetic Identity Abuses by Moving as Fast as Fraudsters

Source: BAI

By the time you finish reading this paragraph, a new synthetic identity may have just been created and approved by a financial institution somewhere in the world. Powered by generative AI, identity fraud is no longer a slow-moving threat. It's fast, scalable, and dangerously convincing.

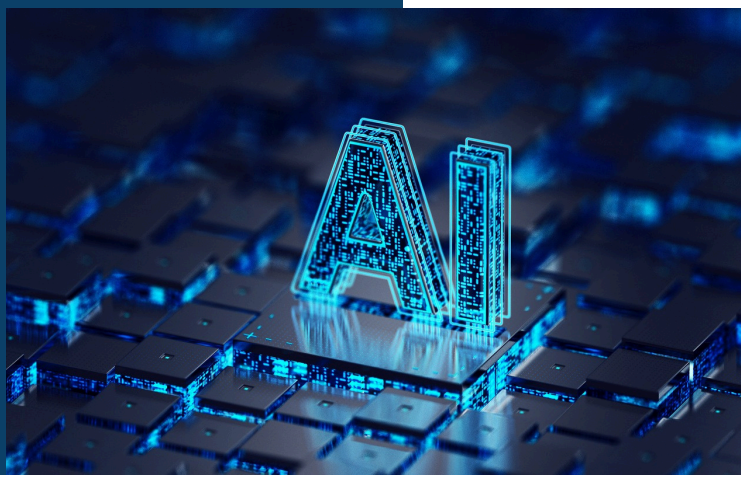
Fraud losses reported by consumers and companies in 2024 topped $12.5 billion, a 25% increase over 2023, according to KPMG.

Much of this surge is driven by deepfakes and AI-generated documents that can mimic real people with alarming accuracy. Criminals can now create entirely fake personas within minutes complete with doctored IDs, AI selfies and scripted responses designed to pass live authentication checks.

And consumers are taking notice. Over three-quarters (78%) of U.S. adults are worried about deepfakes in financial fraud, according to a recent survey by IDScan.net. Yet fewer than half feel confident that today's ID verification systems can stop them.

This technological shift is exposing faults in traditional KYC (Know Your Customer) and AML (Anti-Money Laundering) practices. Static document checks and outdated onboarding protocols are no match for AI systems that can simulate blinking or facial expressions on demand. If fraud is evolving, the tools to stop it must evolve too.

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



On The Right Side of AI

Source: Mastercard

A recent report from Mastercard titled *On the Right Side of AI* highlights the powerful role artificial intelligence is playing in the fight against fraud. According to the report, AI technologies are not only enhancing the speed and accuracy of fraud detection, but they're also helping financial institutions predict and prevent suspicious activity before it impacts customers. This is just one example of how AI is being used to strengthen security and build trust across the financial ecosystem. Community bankers interested in exploring how these innovations can benefit their institutions are encouraged to attend the **CBM AI Summit on October 29 at The Henry Center in Lansing**. The event will showcase practical, real- world applications of AI in community banking, especially those that support fraud prevention, operational efficiency, and customer service.

The rise of large language models (LLMs) and generative AI (Gen AI is enabling organizations to bolster their defenses against an onslaught of payment fraud.

These tools give organizations the capability to sift through a mountain of transactions, identifying subtle patterns that could constitute warning signs, and anticipate fraudsters' future tactics.

But organizations need to maximize the benefits of these AI-powered systems. This means employing data and governance tactics to enhance their effectiveness. They must also find ways to share intelligence securely and responsibly between disparate systems and data sources to make sure they identify genuine threats rather than generate time-wasting false positives.

(Click the heading link to read more.)

Protecting Small Businesses From Check Fraud: Why Positive Pay is a Must-Have Tool

Source: Community Bankers of Michigan

Fraud remains one of the biggest threats facing small businesses today, particularly check fraud, which continues to rise across the country. For community banks looking to strengthen their relationships with local business customers, offering fraud prevention tools like Positive Pay is more important than ever.

Positive Pay is a fraud detection service that helps prevent check fraud by verifying the checks presented for payment match those issued by the business. The business submits a list of approved checks to the bank, including check numbers, amounts, and payees. When a check is presented for payment, the bank cross- references the details. If something doesn't match, the check is flagged for review before any money leaves the account.

This simple yet powerful tool can protect businesses from common threats like:

- Counterfeit checks
- Alter check amounts or payees
- Stolen or washed checks

While larger corporations often have sophisticated fraud prevention teams, small businesses are frequently targeted due to more limited resources and less robust security systems. A single fraudulent check can result in financial loss, operational disruption, and reputational damage. Positive Pay offers a layer of protection that's both proactive and affordable.

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