FRAUD PREVENTION FRIDAY

Community Bankers of Michigan

Friday, June 26, 2026

FinCEN Issues Guidance to Help Financial Institutions Eliminate Fraud Through Information Sharing

Source: U.S. Department of the Treasury

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued updated guidance to clarify how financial institutions can share information with each other about suspected fraud under section 314(b) of the USA PATRIOT Act.

"Americans lose hundreds of billions of dollars to fraud each year. At Treasury, we follow the money, and we know financial institutions are often the first to see suspicious activity in real time. They need the tools to act quickly and share information that can help stop fraud before it spreads," said Secretary of the Treasury Scott Bessent. "Under President Trump and Vice President Vance's leadership, we will continue targeting fraud wherever it occurs and protecting American taxpayers and consumers."

FinCEN's updated guidance clarifies that a financial institution may share information about activity involving suspected fraud, money laundering, terrorist financing,...

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

Top News

Detecting Inbound Bank Fraud and Money Mules

Source: Independent Banker

Community banks have built strong fraud-prevention practices around customers who are sending money out. Tellers are trained to spot unusual wires. Verification thresholds catch large transfers. Conversations at the counter give customers groomed by fraudsters the chance to reconsider transactions. This work has long put community banks on the front lines of fraud prevention, but it captures only one side of the problem.

The other side is inbound activity. Investment fraud, romance scams and online extortion schemes all produce money that must land somewhere before it can move on. Sometimes, it lands at community banks.

A fraud network recruits a money mule, someone to move money on their behalf either knowingly or unknowingly, through a job posting, a relationship or coercion. The mule opens an account, presenting documentation that looks routine. The account receives inbound transfers from victims at other institutions, sent at the fraudster's direction. Within days or hours, the funds move, often to cryptocurrency exchanges or other accounts in a layered chain. By the time the originating bank or law enforcement traces the funds back, the money has typically moved on.

Account opening can move faster at smaller banks than at large institutions, and fraud networks have noticed. Inbound activity runs against a smaller volume base at smaller institutions, which cuts both ways for detection. Much fraud detection technology was built around outbound patterns.

Federal authorities have been documenting the pattern. FinCEN issued an advisory in August 2025 describing how recruited money mules open accounts across multiple institutions to receive and move illicit proceeds.

(Click the heading link to read more.)

Fraud Has Become an Identity Problem

Source: ProSight

Fraud in consumer lending is getting harder to think about the old way. The challenge is no longer just spotting a suspicious transaction. Increasingly, banks have to ask a more basic question first: is the customer really who they appear to be?

Cristian deRitis of Moody's Analytics and Subbu Narayanaswamy of Wells Fargo point to a practical consequence: banks need to rethink where fraud sits in the lending process and how much friction they are willing to impose in trying to stop it.

A few ideas stand out:

The old fraud playbook is under pressure. DeRitis said fraud has always been part of the business, but AI and other technologies have made it "much easier" to commit and harder to detect. Synthetic identity fraud, in particular, is now "much easier, much more diffuse" than in the past. That puts banks in a tricky position. As deRitis put it, "It's a very difficult balancing act." Tighten defenses too much, and legitimate customers struggle to interact. Loosen them too much, and losses rise.

The patterns can look different than they used to. Narayanaswamy pointed to several examples. In synthetic identity fraud, a criminal can pair a real Social Security number and date of birth with a fake name and address, build credit slowly across accounts, then disappear after maxing out the lines. In first-party fraud tied to point-of-sale lending, the identity may be real, but "there is no willingness to pay." And in account takeover, a fraudster can obtain a legitimate customer's credentials ...

(Click the heading link to read more.)

GenAI is the New Weapon in a Fraudster's Arsenal: Is Your Bank Ready?

Source: Plante Moran

Generative AI is reshaping the fraud landscape in banking, enabling attackers to bypass traditional defenses with unprecedented speed and sophistication. Discover evolving threat patterns and practical steps your institution can take to reinforce governance, vendor risk management, and frontline security.

Digital banking has presented new opportunities for smaller banks and financial institutions, but it's also opened the door to unprecedented risks. Today, generative artificial intelligence (GenAI) is giving fraudsters tools that operate at a speed and scale never seen before, enabling them to impersonate customers, deceive employees, and move illicit funds with alarming precision. While leaders have acknowledged the existence of these threats, few recognize how imminent and severe they are — or the steps they should take now to protect their banks.

GenAI's role in modern bank fraud

GenAI has transformed fraud from a manual, time-consuming process into an automated, high-volume operation. Fraudsters can now create lifelike voice clones, deepfake videos, and synthetic identities that pass as real people, making social engineering attacks nearly undetectable. Fake documents such as driver's licenses and Social Security cards can be produced with ease, enabling fraudulent account openings. GenAI can power mass phishing campaigns, generating highly personalized email, SMS messages, and chat scripts at a scale that traditional systems can't keep up with. What once required hours of effort — such as crafting a convincing email from a CFO requesting a wire transfer — can now be replicated thousands of times in just minutes.

(Click the heading link to read more.)

5 Big Challenges Facing BSA and Fraud Teams Today

Source: UBB

Financial crime fighters are dealing with more complex fraud and smarter criminals than ever. Community financial institutions feel significant pressure to operate like national banks with significantly smaller staffing, technology, and budgets.

As a team of former bankers, BSA officers, and bank examiners that partners with community banks every day, these are the five issues we see most often, along with practical steps any institution can take to stay ahead.

1. **Rising Fraud Losses Across Major Channels**

Fraud across check, ACH, and wire transactions continues to increase, and criminals are becoming more adept at exploiting weaknesses.

The FBI's Internet Crime Complaint Center reported more than $10 billion in cyber-enabled losses last year, including more than $3 billion in elder fraud.

Additionally, AI-generated documents, spoofed communications, and deepfake techniques are making it harder for outdated verification processes to keep up. These upticks in losses, paired with the rapidly evolving technology used by bad actors, make it even more difficult for community institutions to keep their customers and members safe.

What You Can Do

(Click the heading link to read more.)