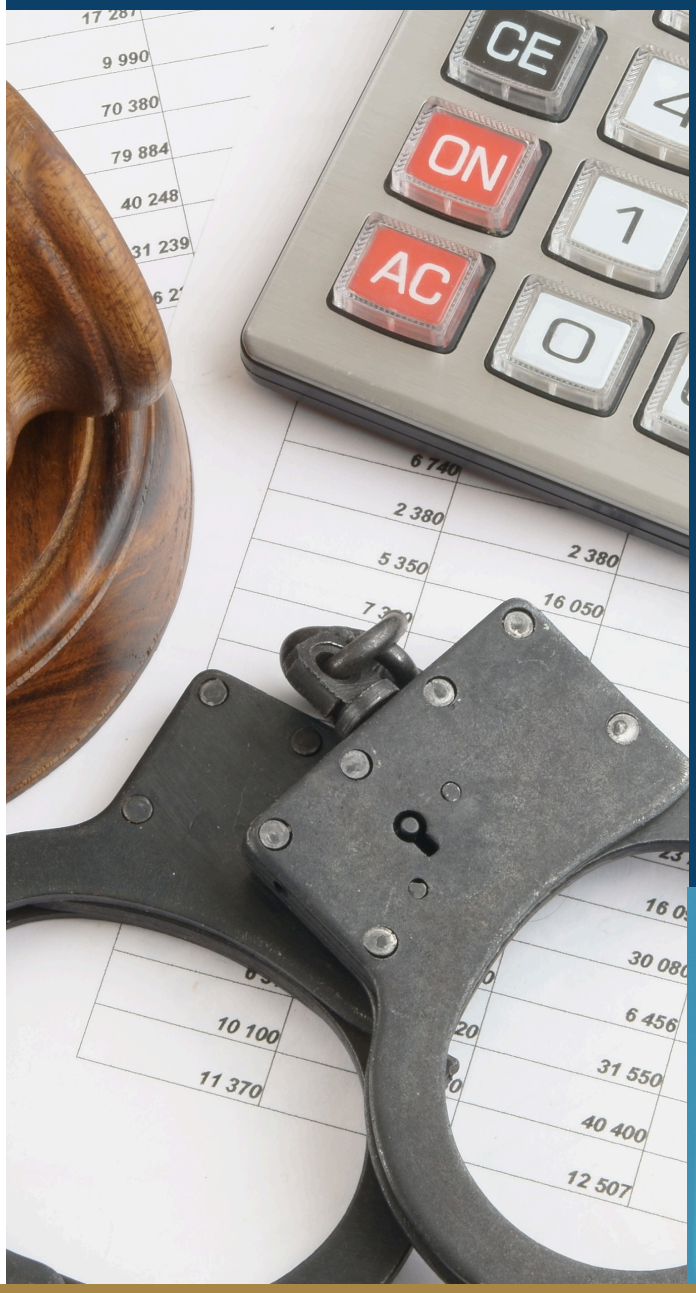
FRAUD PREVENTION FRIDAY

Independent Banks of South Carolina

Friday, August 1, 2025



Top News

- Understanding the Difference Between Fraud and Scam
- Getting Ahead of Cybersecurity Awareness Month

- Fraud Risk Isn't Purely a Financial Issue For Banks
- 5 Ways Real-Time Fraud Detection Can Protect Your Customers

Understanding The Difference Between Fraud and Scam: Insights From The Federal Reserve

Source: ICBA and The Federal Reserve

Yesterday, the CBM hosted its Risk Fraud Forum, where Scott Anchin, Senior Vice President of Strategic Initiatives and Policy at the ICBA, delivered an insightful presentation. He shared key information from the Federal Reserve, highlighting the critical distinctions between fraud and scams, an essential topic for today's banking professionals.

In an increasingly digital world, financial deception is on the rise. The Federal Reserve has issued guidance to help consumers distinguish between fraud and scams, two terms that are often used interchangeably but have essential differences.

What Is Fraud?
Fraud typically involves unauthorized activity that occurs without the victim's knowledge or consent. For example, if someone steals your credit card number and makes purchases without your permission, that's fraud. You didn't knowingly participate in the transaction, and you're a victim of identity theft or data breach.

The Federal Reserve emphasizes that fraud often involves:

- Stolen personal or financial information
- Unauthorized transactions
- No direct interaction with the perpetrator

What Is a Scam?

A scam, on the other hand, involves deception that tricks the victim into willingly providing information or money.

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

Getting Ahead of Cybersecurity Awareness Month: A Guide for Community Bankers

Source: Community Bankers of Michigan

October is just around the corner, and with it comes Cybersecurity Awareness Month a critical opportunity for community banks to reinforce their commitment to protecting customer data, strengthening internal defenses, and fostering a culture of cyber vigilance.

As cyber threats grow more sophisticated and frequent, community banks often seen as prime targets due to limited resources must take proactive steps to prepare. Here's how your institution can get a head start. **1.**

(1) Assess Your Current Cybersecurity Posture

Start with a comprehensive risk assessment. Review your:

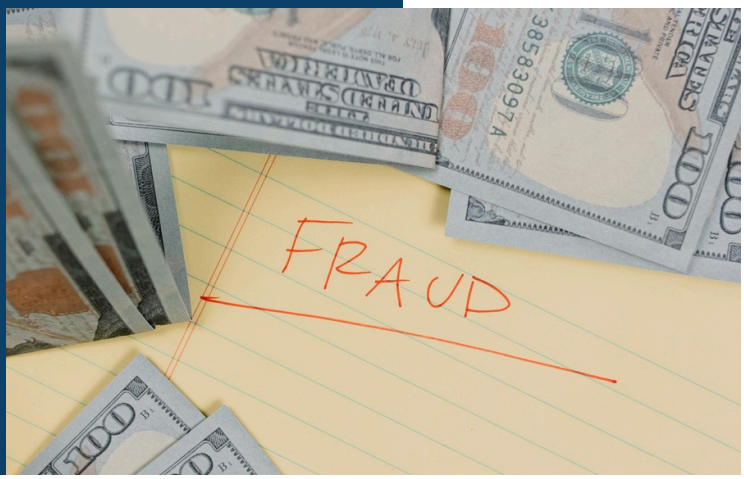
- Incident response plan: Is it up to date and tested?
- Employee training programs: Are staff aware of phishing tactics and social engineering?
- Vendor management: Are third-party partners secure?
- Access controls: Are permissions aligned with job roles?

Use this time to identify gaps and prioritize remediation efforts.

(2) **Plan Awareness Campaigns for Staff and Customers**

Cybersecurity Awareness Month is the perfect time to educate and engage.

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



Fraud Risk Isn't Purely a Financial Issue For Banks

Source: BAI

Fraud has long been a challenge in the financial sector, but today's environment presents unprecedented risks. Record-high transaction volumes and a surge in first-party fraud are putting immense pressure on banks to do more with fewer resources, especially when it comes to resolving disputes.

As recently as 2023, 79% of community financial institution leaders reported direct fraud losses exceeding $500,000. This figure doesn't even account for the operational costs of investigating and processing dispute claims.

While fraud is often viewed as a purely financial issue, the reality is that its impact goes far beyond the bottom line because how bankers respond to fraud and resolve disputes can significantly influence the quality of the customer relationship. In fact, a recent consumer banking survey revealed that poorly handled fraud incidents are among the top reasons customers switch financial institutions. With many disputes taking 45–90 days to resolve, it's no surprise that customers grow frustrated with prolonged timelines to resolving legitimate disputes.

The positive news for bankers is that, when handled correctly, these incidents also present a unique opportunity to build trust with customers and actually strengthen customer loyalty. According to a J.D. Power survey, 92% of customers who felt supported during a fraud incident said they were likely to stay with their bank afterward.

(Click the heading link to read more.)

5 Ways Real-Time Fraud Detection Can Protect Your Customers

Source: PCBB's BID Daily Newsletter

Real-time fraud detection relies on new technologies such as artificial intelligence (AI) and predictive analytics to track and flag unusual activity, machine learning (ML) to detect anomalies and adapt to evolving threats, and behavioral biometrics to identify differences in user behavior such as typing speed, mouse movements, and device usage. Adopting real-time fraud detection strategies can deliver substantial benefits to CFIs, such as:

- Enhancing the customer experience. Early detection of fraudulent activity and a quick response help build customer confidence. Moreover, by reducing false positives, fewer legitimate customers face unnecessary hurdles.
- Protecting from fraud-related losses. By identifying suspicious transactions or activities in real time, institutions can prevent financial and data losses before they escalate. What's more, they can reduce the costs associated with investigating and settling fraudulent transactions.
- Keeping up with fast-evolving fraud methods. Many real-time systems collect vast amounts of data and mine it for insights to predict new lines of attack from fraudsters.
- Shifting focus from fraud to growth. Using automated fraud detection and response strategies can free up an institution's resources to focus on its core competencies.

(Click the heading link to read more.)