

FRAUD PREVENTION FRIDAY



Friday, October 2, 2026



ICBA Publishes Cyber Insurance Resource for Community Bankers

Source: ICBA

ICBA released a white paper to help community banks address the challenges of securing cyber insurance coverage, with a particular focus on artificial intelligence issues.

Developed by members of the ICBA Cyber and Data Security Subcommittee, "*Safeguarding Resilience: Navigating Cyber Insurance in the Age of Artificial Intelligence*":

- Says AI-driven attacks may not be explicitly covered under standard policy language.
- Explains that vendor-embedded AI tools introduce additional exposures that are often invisible to underwriters and absent from policy terms.
- Offers recommendations and a checklist of 30 questions community bankers should raise directly with their insurers to identify coverage gaps before an incident occurs.

(Click the heading link to read more.)

Top News

- [ICBA Publishes Cyber Insurance Resource for Community Bankers](#)
- [Help Shape the Fight Against Payments Fraud](#)
- [Protecting Customers During Stressful Moments: Understanding Scam Risk Across Customer Segments](#)
- [How Financial Institutions Can Help Accountholders Avoid Bank Impersonation Scams](#)
- [Your Verification Has Amnesia - Fraud Remembers](#)



Help Shape the Fight Against Payments Fraud

Source: The Federal Reserve Financial Services

Fraud remains one of the most pressing challenges facing financial institutions, and community banks are on the front lines of protecting consumers and businesses from increasingly sophisticated scams. To help address these growing threats, the Federal Reserve Financial Services is seeking input from U.S.-based depository institutions through its Fraud Mitigation Survey.

The survey is intended for organizations that provide payment services to retail or business customers, with participants ideally involved in fraud detection, prevention, risk management, or payment operations. Feedback gathered through the survey will help the Federal Reserve better understand current fraud trends, emerging risks, and the challenges financial institutions face in safeguarding their customers.

Survey questions focus on five key areas:

- Fraud trends
- Key priorities and focus areas
- FRFS products and services
- Emerging concerns and risks
- Industry engagement and collaboration

Community banks play a critical role in identifying fraud patterns and developing effective mitigation strategies. By sharing your institution's experiences and insights, you can help inform future fraud prevention initiatives, resources, and industry efforts to strengthen the safety and security of the U.S. payments system.

If your institution has team members responsible for fraud monitoring, mitigation, or payment operations, please consider participating. Your feedback will help ensure the unique perspectives and challenges facing community banks are represented in ongoing efforts to combat fraud and protect customers nationwide.

(Click the heading link to read more.)



Protecting Customers During Stressful Moments: Understanding Scam Risk Across Customer Segments

Source: The Federal Reserve FedPayments Improvement

We all experience moments in life where we are more vulnerable to scams. These moments could include buying a home, being a victim of a natural disaster, or coping with the loss of a loved one. During these moments, we may experience heightened stress and reduce our attention to risk. Unfortunately, criminals know this. Criminals can more effectively perpetrate payment scams when they deliberately target people when they are vulnerable, exploiting urgency, distraction, and lowered skepticism.

This article, part of the series Understanding Scam Risk Across Customer Segments, explores scam risks impacting people at times of increased vulnerability and what financial institutions can do to protect their customers through timely education, outreach and support.

Stress Disrupts Decision Making

Stress can reduce the mental capacity we rely on for judgment, skepticism, and attention to red flags.

During stressful times:

- The brain shifts into rapid response mode, prioritizing urgency over analysis.
- Emotional load reduces working memory, making it harder to assess risk or notice inconsistencies.
- People become more likely to comply with authoritative or urgent-sounding requests.
- Quick decisions replace slower, more deliberate thinking.

(Click the heading link to read more.)



How Financial Institutions Can Help Accountholders Avoid Bank Impersonation Scams

Source: SHAZAM

Phone spoofing technology has made it easier for fraudsters to appear legitimate. An incoming call may display a familiar phone number, the caller may sound professional or the situation may seem urgent. That is what makes bank impersonation scams so effective.

As these scams continue to evolve, financial institutions have an opportunity to help accountholders recognize the warning signs before fraud occurs.

How do bank impersonation scams work?

A bank impersonation scam often begins with an unexpected phone call or text message claiming there is a problem with an account. The fraudster may report suspicious activity, a compromised card or another security concern requiring immediate attention.

To make the interaction appear legitimate, scammers frequently use caller ID spoofing technology to display a financial institution's phone number. The fraudster's goal is usually to gain access to account credentials (like usernames and passwords), obtain personal information or convince the accountholder to move money to an account controlled by the scammer.

What warning signs should accountholders watch for?

While scam tactics vary, most bank impersonation scams share several common red flags.

Unsolicited contact about an urgent issue

Fraudsters create a sense of urgency to pressure accountholders into acting quickly. They may claim an account has been compromised or that funds are at risk. Counter this by encouraging accountholders to pause and verify the situation before taking any action.

(Click the heading link to read more.)



Your Verification Has Amnesia – Fraud Remembers

Source: Veriff

Some identities never really disappear. They keep coming back to apply again and again. The same stolen document, the same face, the same device; rejected on one platform, then recycled on the next. And the next. We call them zombie identities. And traditional onboarding checks weren't built to recognize a fraudster coming back for another attempt.

That's the problem this piece opens up. The full numbers arrive in the Identity Fraud Report 2027, but the pattern is already visible in the data we have.

Fraud isn't new. It's persistent.

According to the Veriff Identity Fraud Report 2026, 4.18% of all verification attempts in 2025 were flagged as fraudulent: roughly 1 in every 25, and the rate has held above 4% for the third year in a row. Impersonation accounted for more than 85% of those attempts. E-commerce marketplaces hit a 19.2% net fraud rate. Financial services crossed 5.5%.

These aren't isolated incidents. And a steady rate hides something our fraud teams see every day: the same identities, documents, and faces cycling through verification, again and again, across platforms and time.

Why zombie identities keep working

A verified identity is a proven asset. Once a document clears a check somewhere, it has value. That value gets reused. The same document template comes back with a new name and date of birth. The same selfie appears across different accounts. The same device runs dozens, sometimes hundreds, of sessions. And a rejection isn't the end, either. It's feedback: fraudsters adjust the lighting, swap the document, change the device, and try again.

(Click the heading link to read more.)