FRAUD PREVENTION FRIDAY

Independent Banks of South Carolina

Friday, August 22, 2025

ICBA Urging Community Banker Grassroots Letters on Fraud

Source: ICBA Newswatch Today

ICBA is calling on community bankers to use its newly published grassroots guide to submit comment letters on an ICBA-supported interagency request for information on mitigating payments fraud.

The FDIC, Federal Reserve, and OCC are requesting input on actions they could take to help consumers, businesses, and financial institutions mitigate check, ACH, wire, and instant payments fraud. Comments are due by Sept. 18.

Key Issue Areas: The agencies requested input on five potential areas for improvement and collaboration:

- External collaboration among the agencies, Federal Reserve Banks, and industry stakeholders.
- Consumer, business, and industry education.
- Regulation and supervision to mitigate payments fraud.
- Data collection and information sharing.
- Federal Reserve Bank operator tools and services.

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

Top News

Federal Reserve Unveils Two Online Toolkits for Scams and Check Fraud Mitigation

Source: The Federal Reserve FedPayments Improvement

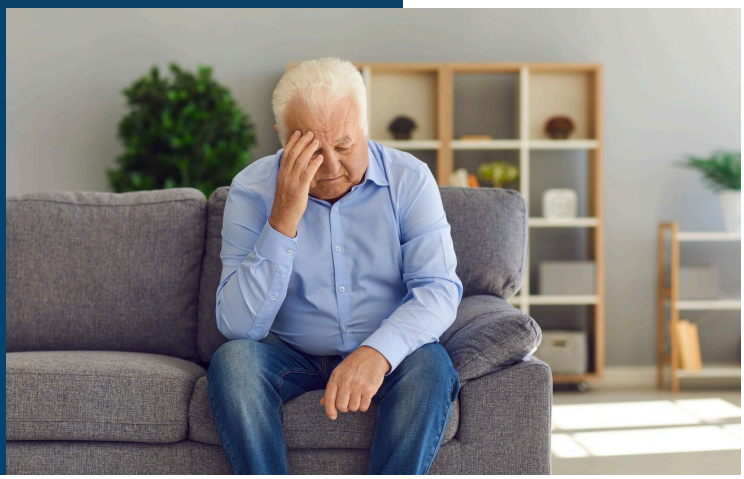
Payments fraud continues to grow and impact individuals and organizations alike. According to the Federal Trade Commission, consumers reported losing more than $12.5 billion to fraud and scams in 2024, up 25% from the prior year. Additionally, check fraud was among the primary drivers of fraud events in 2024 despite declining check volumes.

The Federal Reserve has released two new toolkits — the Scams Mitigation Toolkit and the Check Fraud Mitigation Toolkit. As online repositories of insights and downloadable resources, the toolkits are intended to support education and increase awareness about scams and check fraud, enable the payments industry to better identify and fight them, and foster industry collaboration on fraud and scams mitigation. These toolkits complement a Synthetic Identity Fraud Mitigation Toolkit that was released in 2022.

The initial releases of the Scams Mitigation Toolkit and Check Fraud Mitigation Toolkit focus on building foundational knowledge about different types of scams and check fraud, the tactics and human vulnerabilities that often enable these schemes to succeed, and common scenarios that financial institutions, service providers, other businesses, and individuals may encounter.

A scam is defined as the use of deception or manipulation intended to achieve financial gain. This growing, evolving threat impacts individuals, businesses and entire economies. Consequences include financial, emotional and psychological tolls. In some cases, the stolen money fuels global organized crime.

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



FTC Data Show a More Than Four-Fold Increase in Reports of Impersonation Scammers Stealing Tens and Even Hundreds of Thousands From Older Adults

Source: Federal Trade Commission

New analysis from the Federal Trade Commission shows a more than four-fold increase since 2020 in reports from older adults who say they lost $10,000 or more— sometimes their entire life savings—to scammers who impersonate trusted government agencies or businesses to convince consumers to transfer money to protect it, when in reality the scammers want to steal it.

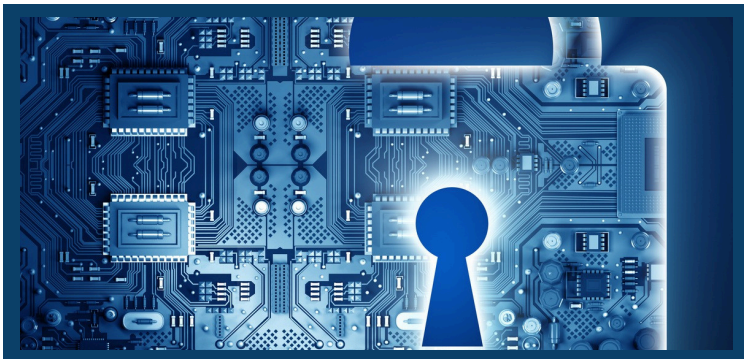
The FTC's latest *Consumer Protection Data Spotlight* shows a huge jump in losses reported by people 60 and over to these types of impersonation scams in the last four years. Most notably, combined losses reported by older adults who lost more than $100,000 increased eight- fold, from $55 million in 2020 to $445 million in 2024. While younger consumers have also reported these scams, older adults were much more likely to report these extraordinarily high losses.

The scams generally involve someone contacting consumers to alert them to a fake and urgent problem and then proceeding to try to persuade them to transfer their money to "keep it safe" or for some other false reason. In reality, the money is being sent to the scammers.

The lies these scammers tell generally take three forms:

- Lie #1: Someone is using your accounts: The scammers claim to be from your bank or a well-known company like Amazon and are contacting you to flag suspicious activity on your account;

(Click the heading link to read more.)



Win With Defense: How FIs Can Foil Cybercriminals

Source: BAI

Community banks and credit unions pride themselves on close customer relationships, personalized service, and deep community ties. While the smaller size of these financial institutions is often a significant competitive advantage, it also makes them an attractive target for cyberattacks. Leaders of these institutions understand that they can't effectively defend against evolving cyber threats on their own.

Cybercriminals target community banks and credit unions precisely because they lack the resources and sophisticated defenses of larger institutions. Bad actors view small FIs as entry points to the broader financial system. Steal credentials from a credit union, and bad actors believe they'll gain access to correspondent banking relationships, payment networks or customer data that open doors to much larger targets.

The question is not when a cyberattack will happen. It's whether you'll be ready when it does. The good news is that effective cybersecurity is not about unlimited technology budgets; it's about a systematic approach, targeted investments, and strategic relationships with partners whose reputations and business models depend on keeping clients secure.

A Zero Trust security strategy—"trust no one, validate everything"—is foundational to modern cybersecurity. It means every access request, inside or outside your network, must be verified before access is granted, with vigilant deployment of authentication and access controls. Multi-factor authentication (MFA) for all employees—especially those with access to sensitive systems or customer data—significantly reduces the risk of credential theft. Role-based access controls (RBAC), PIN-based teller authentication and dual control measures for high-risk operations ensure employees have appropriate-but-limited access to systems required for their work, minimizing the potential "blast radius" from a breach.

(Click the heading link to read more.)