FRAUD PREVENTION FRIDAY

Independent Banks of South Carolina

Friday, June 27, 2025

Banks Can Use CFPB's Resources to Help Older Customers

Source: CFPB

Did you know the Consumer Financial Protection Bureau's (CFPB) Office for Older Americans offers free resources that may be helpful for bank staff, including reports, advisories, and consumer education tools? You can use these materials to educate your staff and customers about elder financial exploitation.

Consumer education tools:

- Banks can make available CFPB's Managing Someone Else's Money guides to help financial caregivers understand their role as agent under a power of attorney, a guardian or conservator, trustee, Social Security representative payee or Veterans Affairs fiduciary.

- Staff can volunteer to share the Money Smart for Older Adults program with older customers and caregivers to help them make informed financial decisions and protect against scams. The program includes an Instructor Guide, PowerPoint slides, and a take-home Resource Guide.

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

Top News

- Banks Can Use CFPB's Resources to Help Older Customers
- NTAS Bulletin Highlights Rising Cyber, Terror Threats to U.S. Critical Infrastructure From Iran-Linked Hackers
- Smart Friction's Role in Better Cybersecurity
- Is This The Calm Before The Storm?
- Federal Bank Regulatory Agencies Seek Comment to Address Payments and Check Fraud

NTAS Bulletin Highlights Rising Cyber, Terror Threats to U.S. Critical Infrastructure From Iran-Linked Hackers

Source: Industrial Cyber

The latest National Terrorism Advisory System bulletin from the U.S. Department of Homeland Security warns community banks about the rising threat of cyberattacks from Iran-linked hackers targeting critical infrastructure. As geopolitical tensions escalate, the risk of both low-level and sophisticated cyber intrusions increases.

Community bankers must stay vigilant, strengthening their own institutions and their networks of IT partners to ensure robust cybersecurity. The U.S. Department of Homeland Security (DHS) on Sunday issued a National Terrorism Advisory System(NTAS) bulletin warning that the ongoing conflict with Iran is fueling a heightened threat environment inside the U.S. The NTAS bulletin noted that pro-Iranian hacktivists are likely to launch low-level cyberattacks against U.S. networks, while Iran-linked cyber operators may attempt more targeted intrusions.

The bulletin also flagged Iran's longstanding intent to retaliate against U.S. government officials it holds responsible for the January 2020 killing of a top Iranian military commander. DHS noted that the threat of violence from domestic extremists could intensify if Iran's leadership issues a religious decree urging attacks on U.S. soil. Recent domestic terror incidents driven by anti-Semitic and anti-Israel sentiment underscore the risk of additional plots sparked by the Israel-Iran conflict.

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

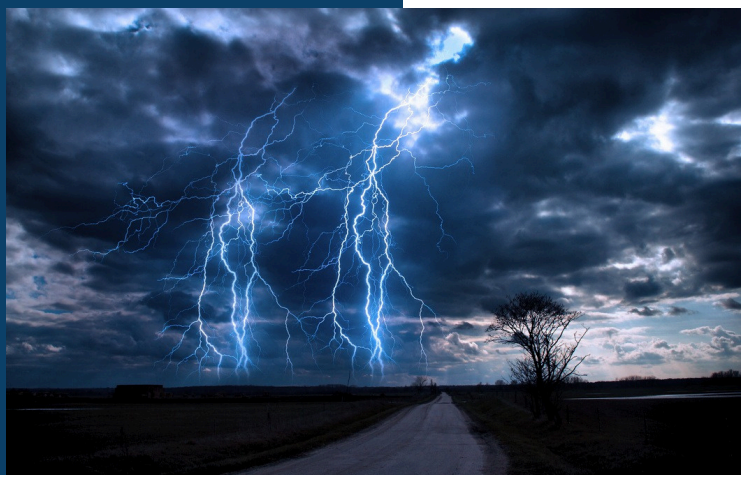
Smart Friction's Role in Better Cybersecurity

Source: PCBB's BID Daily Newsletter

Financial institutions already have security measures in place to guard against fraud, with certain activities triggering fraud alerts. Smart friction uses AI to take it a step further by identifying potentially suspicious activity and then applying additional security measures like extra confirmations. This means analyzing factors within authentication and transaction processing — like source devices, locations, transaction types, and behaviors — and then introducing interventions when things look suspicious.

For instance, a legitimate customer who logs into their banking app from their usual device and location can be authenticated easily with their typical login method. On the other hand, a user attempting to access the same account during overnight hours from an unfamiliar device with a foreign IP address would be faced with a myriad of hurdles to log in. These could include requiring biometric authentication or validation codes through push notifications to the account owner's mobile device. In the unlikely event that the bad actor is able to gain access, any transactions they try to process might be subject to temporary holds while the financial institution attempts to contact the customer and verify the transaction was made by them. This adds a lot more friction, but it also adds a lot more security. The goal is to keep bad actors out of your community financial institution's (CFI's) systems while continuing to give your real customers the high level of service they demand.

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



Is This The Calm Before The Storm?

Source: LexisNexis

After several years of skyrocketing digital fraud (as tracked through LexisNexis® Digital Identity Network® solution), data shows the rate of attacks by humans rising by just 1% last year. That said, the number of attacks is still increasing, and organizations that become complacent are putting themselves at risk. Challenges are still multiplying around the world, and in the communications, mobile and media sector attack rates were up 15% year- over-year (YOY). In other sectors, there was no significant increase in attack rate, suggesting that fraudsters are avoiding organizations with more sophisticated defenses. But the attack-rate slowdown we're seeing might be short-lived; fraudsters and scammers are likely retrenching against heightened security. In this report, we explore the tangled web of scams and mules in depth, and show how our data reveals telltale patterns of scam and mule activity. And we'll demonstrate the value of collaboration as the only way to reliably reduce fraud in today's complex environment. Scams dominate global headlines, but organizations today struggle with a wide range of attacks, including the use of compromised or synthetic identities and payment credentials, bonus abuse and first-party fraud. In our detailed look at the relative incidence of these fraud classifications, first-party fraud was the number one reported category. On the other side of the equation, enterprises that have invested in modern, sophisticated defenses are enjoying success.

(Click the heading link to read more.)

Federal Bank Regulatory Agencies Seek Comment to Address Payments and Check Fraud

Source: Board of Governors of the Federal Reserve System

Earlier this month, the federal bank regulatory agencies announced a request for comment on potential actions to help consumers, businesses, and financial institutions mitigate risk of payments fraud, with a particular focus on check fraud. For purposes of the request for information, payments fraud generally refers to the use of illegal means to make or receive payments for personal gain, including scams. Because payments fraud may involve multiple institutions and payment methods, no single agency or private-sector entity can address payments fraud on its own. Therefore, the agencies are seeking public comment on discrete actions, collectively or independently, to mitigate payments fraud, including check fraud, within their respective bank regulation and payments authorities. Input is requested on five potential areas for improvement and collaboration:

- External collaboration among the agencies, Federal Reserve Banks, and industry stakeholders;
- Consumer, business, and industry education by the agencies and Federal Reserve Banks to educate about payments fraud;
- Regulation and supervision to mitigate payments fraud, including opportunities the Board may have related to check fraud;
- Payments fraud data collection and information sharing; and
- Federal Reserve Banks' operator tools and services to reduce payments fraud.

(Click the heading link to read more.)