FRAUD PREVENTION FRIDAY

Independent Banks of South Carolina

Friday, October 10, 2025

Four Banks, Four Failures: Strengthening Internal Controls for Fraud Prevention

Source: Ncontracts

Fraud has already claimed two banks, and 2025 is farfromover. The January collapse of Chicago's Pulaski Savings Bank, followed by June's failure of The Santa Anna National Bank in Texas, marks a disturbing acceleration in fraud- related bank failures.

These financial institutions (FIs) are part of an alarming pattern that has seen four banks fail due to inadequate internal controls for banks in just four years. Each failure was preventable, each more costly than necessary, and each shared control weaknesses that many community banks would recognize in their own operations.

Now is the time for FIs to be on high alert and strengthen their internal controls to prevent similar fraud-related incidents from happening at their institutions. Building a strong foundation and maintaining continuous monitoring can mean the difference between a thriving institution and one on the brink of failure.

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

Top News

CISA Shares Lessons Learned from an Incident Response Engagement

Source: Cybersecurity & Infrastructure Security Agency (CISA)

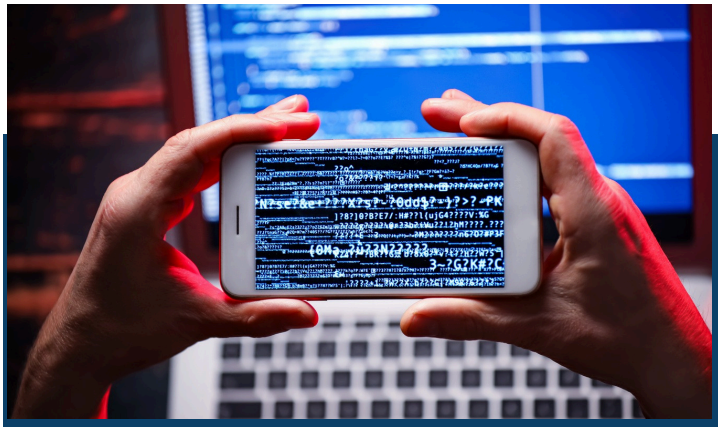
The Cybersecurity and Infrastructure Security Agency (CISA) is releasing this Cybersecurity Advisory to highlight lessons learned from an incident response engagement CISA conducted at a U.S. federal civilian executive branch (FCEB) agency. CISA is publicizing this advisory to reinforce the importance of prompt patching, as well as preparing for incidents by practicing incident response plans and by implementing logging and aggregating logs in a centralized out-of-band location.

CISA is also raising awareness about the tactics, techniques, and procedures (TTPs) employed by these cyber threat actors to help organizations safeguard against similar exploits. CISA began incident response efforts at an FCEB agency after the agency identified potential malicious activity through security alerts generated by the agency's endpoint detection and response (EDR) tool. CISA discovered cyber threat actors compromised the agency by exploiting CVE-2024-36401 in a GeoServer about three weeks prior to the EDR alerts. Over the three-week period, the cyber threat actors gained separate initial access to a second GeoServer via the same vulnerability and moved laterally to two other servers.

Leveraging insights CISA gleaned from the organization's security posture and response, CISA is sharing lessons learned for organizations to mitigate similar compromises (see Lessons Learned for more details):

1. Vulnerabilities were not promptly remediated.
   a. The cyber threat actors exploited **CVE-2024**-36401 for initial access on two GeoServers.

(Click the heading link to read more.)



ICBA: Community Banks Lead the Fight Against Fraud

Source: ICBA

ICBA told Congress that community banks are on the front lines of fraud mitigation and are leading the response but cannot solve the problem alone.

In a statement for the record prior to a House Financial Services Committee subcommittee hearing on fraud, ICBA said:

- Two types of fraud have become increasingly prevalent and can have crippling effects on victims: check fraud and the financial abuse of U.S. seniors.
- New or revised supervisory guidance that is particularly burdensome could impact community banks' ability to effectively prevent, detect, or mitigate fraud by forcing resources to be redirected.
- Community banks would benefit from automated data collection, analysis, and reporting tools that are integrated with services they already use and do not carry additional costs.

In the statement, ICBA listed its ongoing check fraud-mitigation efforts, including:

- ICBA's Fraud Task Force, which brings together community banks and state associations from across the country to share information, build relationships with regulators, and collaboratively develop resources.
- ICBA's partnership with the U.S. Postal Inspection Service, which includes a customizable news release via ICBA's Marketing Resource Center and a check fraud prevention flyer community bankers can distribute to customers.

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

From Digits to Data: How ESIM Numbers Fuel Account Takeovers

Source: Q6 Cyber

A threat actor who goes by the moniker "crdEPATAGE" on the Russian-speaking underground forum XSS1 shared a novel step-by-step method for taking over victims' bank accounts. This reputable actor specializes in developing bypass techniques and schemes targeting U.S. financial institutions.

Traditional PII-based banking fraud workflows typically begin with the acquisition of a victim's personally identifiable information (PII), followed by social engineering and attempts to acquire a phone number to bypass multi-factor authentication (MFA) controls.

In contrast, the novel method described by crdEPATAGE starts backwards - with an eSIM-based phone number purchased through providers such as usmobile.com and then checks whether that number was previously associated with a real individual. If a match is found, the actor works backward to reconstruct the full identity profile, building from the phone number to the reconstructed full PII profile including name, address, date of birth, SSN, and other sensitive information. Since financial institutions often rely on credit agency–linked identity data for user verification, this approach gives threat actors a powerful advantage, bypassing authentication checks and gaining access to accounts without requiring control of the victim's device or inbox.

Here's how the process works, step by step:

1. Acquire a Phone Number - Purchase and activate amobile number via eSIM through services such as usmobile.com. The number becomes the starting point for the identity-building process.

2.Check for Previous Ownership - Run the acquired number through background check services (e.g., TruthFinder, 2 FamilyTreeNow 3) to determine whether it was ever linked to a real person. If results indicate a past owner with associated identity details, continue to the next step.

(Click the heading link to read more.)

Unmasking a Threat to KYC

Source: Q6 Cyber

In 2025, AI-driven scams targeting Know Your Customer (KYC) controls have become a growing concern, with deepfakes now accounting for one in every 20 identity verification failures.1 In addition, according to AuthenticID's 2025 State of Identity Fraud Report, 46% of surveyed businesses reported a year-over-year increase in deepfake and generative AI fraud.2 This is the last installment in our deepfake series.

As AI-driven fraud accelerates, it's become a top concern for security experts. To counter this growing risk, researchers suggest that integrating advanced biometric verification with AI-powered detection algorithms could arm defenses against video-based manipulation by nearly 40%.

Increased investment in deepfake detection has fueled market growth, with recent analyses projecting the sector to exceed $3.5 billion by the end of 2025.4 Another forecast estimates the broader deepfake detection market will reach $15.7 billion by 2026.

Although cybercriminals continue to abuse deepfake technology for KYC, some have commented that organizations have seemingly implemented measures to better detect these attempts, making it more difficult and complicated for cybercriminals to bypass these controls.

As such, cybercriminals are exploring more creative ways to authenticate. We have observed an interest in using high quality silicone or latex masks, noting they too can be used to bypass KYC. Although the use of hyper realistic masks by criminals is not a new tactic, it continues to play a role in crime. In one recent high-profile case involving the murder of two Democratic lawmakers, the suspect impersonated a police officer reportedly wearing a hyper realistic face mask.

(Click the heading link to read more.)