FRAUD PREVENTION FRIDAY

Friday, October 18, 2024

Check Fraud: Detection Mechanisms

This document explains some of the potential technology solutions and operational mechanisms that are available to community banks to detect instances of check fraud. It is intended to be brief and to serve as a reference for community banks to evaluate tools and leverage internal practices to identify and prevent check fraud.

Effectively detecting check fraud requires a layered approach that combines both software and manual processes. Every community bank's approach will differ and should be guided by deliberate strategic planning that incorporates a cost-benefit analysis of all available mechanisms, a historical loss analysis, and the parameters of each bank's compliance program.

This document was developed by community bankers working together as part of ICBA's Check Fraud Task Force. This document is for general information purposes and is not intended to be, and should not be taken as, legal advice, an endorsement of any specific company or product, or a comprehensive treatment of the subject matter.

Top News

BankOnIT CEO Update: Cybersecurity Risks

Cyber risks pose significant financial sector and broader U.S. economy threats, according to the Spring 2024 Semiannual Risk Profile released by the OCC. Cyberattacks continue to evolve and become more sophisticated and pervasive throughout the financial sector. The OCC report further states threat actors continue to exploit publicly known software vulnerabilities and weak authentication controls at targeted organizations, including banks and financial service providers.

The OCC recently released their Bank Supervision plan for 2025 and provided the following areas of focus:

- Examiners will continue to focus on the adequacy of banks' preventative controls, incident response, data recovery, and operational resilience.
- Examinations will emphasize incident response, backup, and operational resilience capabilities to withstand or recover from cyberattacks, especially for critical operations.
- Examiners will also consider cyber intelligence gathering, sharing, and analysis; threat and vulnerability detection; and strong authentication and access controls, including the use of multi-factor authentication, to include third-party access management, network management, and data management.

(Click on the link in the title to continue reading.)

This Week's Top Threats - Cybersecurity Awareness Tips

Cybercriminals continue to target vulnerable individuals and organizations through a variety of sophisticated fraud campaigns. Common threats include account takeover, call center fraud, CEO impersonation, credential pharming, customer validation scams, employee impersonation, fake invoices, and fraudulent gift card requests. Other tactics, such as new account fraud, online account hijacking, wire transfer fraud, and unauthorized withdrawals and enrollments, are also on the rise. Community banks play a vital role in educating their customers to stay safe from these threats by regularly sharing tips on identifying phishing emails and suspicious phone calls and verifying the legitimacy of requests. Hosting webinars, sending regular email alerts, and posting on social media about the latest fraud tactics can raise awareness. Additionally, banks should encourage customers to use multi-factor authentication, monitor their accounts for unusual activity, and report any suspicious behavior immediately. Offering in-branch training sessions or personalized consultations can further empower customers to recognize and avoid scams.

Safety Concern Related to Recent Trend in Financial Institution Fraud Scheme

The Federal Bureau of Investigation (FBI) warns the public of a fraudulent scheme in which scammers impersonate bank representatives, hereinafter "impersonators," to fraudulently obtain bank cards (with "chips") from bank customers. The safety concern is the impersonators are hiring accomplices to come to the customer's home.

Bank customers are contacted by phone from a number that caller ID indicates is from their bank. The impersonator then asks about recent transactions to lead the customer to believe there is a fraudulent activity involving their account. Bank customers are then advised to cut up their bank card but are instructed to leave the chip intact for return to the bank. Next, the impersonator arranges for an accomplice, also allegedly "from the bank," to pick up the bank card (with chip intact) from the customer's residence. If the impersonators do not currently have the customer's PIN, the accomplice or impersonator will use social engineering techniques to obtain this from the customer. It has been reported that if the customer has not already done so, the accomplice may "assist" the customer by cutting the card and leaving the chip intact before departing with the remnants. With the chip and PIN, the impersonators can steal funds from the bank customer's account.

It is unknown how the impersonators are obtaining personal information (name, address, and bank account information.) At this time, it is not believed specific demographics are being targeted.

The FBI requests these fraudulent or suspicious activities are reported to the FBIIC3 at www.ic3.gov as quickly as possible. Be sure to include:

- How the complainant was contacted, including phone numbers.
- Any aliases utilized.
- Please include the keywords #BankChipHack.

Those affected should also contact your financial institution account providersimmediately to regain control of your accounts, change passwords, and place alertson your accounts for suspicious login attempts and/or transactions.

Enhancing Customer Protection: Encouraging the Use of a Trusted Contact Form

As community bankers, we strive to provide exceptional financial services while ensuring the safety and security of our customers' assets. One important tool that can enhance this protection, particularly for elderly clients or those at risk of financial exploitation, is the **Trusted Contact Form**. This simple but crucial document allows customers to designate a trusted individual with whom their financial information can be shared in case of emergencies or suspected fraud. Encouraging your customers to complete this form not only strengthens the bond of trust between the bank and the customer but also adds a vital layer of protection against scams, fraud, and financial abuse.

Financial fraud, particularly targeting vulnerable populations like seniors, has become increasingly sophisticated. By completing a **Trusted Contact Form**, your customers give the bank permission to reach out to a designated person if there are signs of suspicious activity on their account, if the customer cannot be reached, or if there are concerns about their well-being. This could be a family member, close friend, or any individual the customer feels confident in handling sensitive financial information responsibly. Having this safeguard in place ensures potential problems can be addressed promptly, potentially stopping fraud or exploitation before it can escalate.

Benefits to Your Customers

1. *Added Security*: A trusted contact provides an extra layer of oversight for their financial accounts, particularly during emergencies.
2. *Peace of Mind*: Customers can feel reassured knowing someone they trust will be notified in the event of irregular account activity or suspected fraud.
3. *Protection from Financial Abuse*: For elderly customers, those experiencing declining cognitive abilities, or individuals living alone, having a trusted contact can prevent financial exploitation by allowing the bank to quickly involve someone who can intervene.
4. *Safeguard in Times of Crisis*: Life events like illness or natural disasters can leave customers temporarily unavailable. A trusted contact can assist in ensuring financial matters are handled appropriately during such times.

(Continued on next page.)

Check Fraud - Orchestrated Attacks and the Rise of Mule Accounts in Community Banks

Recent news has highlighted a concerning trend in the world of financial fraud: so-called "glitches", the recent viral trend on social media that encouraged people to deposit fake checks for large sums of money, exploiting a financial institution's (FI) fund availability glitch, and they cash out the funds immediately before those checks bounced. These aren't free or infinite money glitches. There isn't a cheat code for free money like there was in your favorite video game—it's modern-day check fraud. And the sense of gamification is purposeful. Bad actors use the feeling of gamification to diminish the perceived seriousness of what people are engaging in. These memes and other social media tactics that go viral amplify their message to create chaos and flash fraud. It is my opinion that organized fraud rings are targeting FIs to exploit and perpetrate widespread check fraud, amplify via social to create chaos, and use this chaos to hide amongst those who piled on. While these high-profile incidents have predominantly targeted larger FIs, community banks, credit unions, and regional banks are not immune. In fact, the nature of these orchestrated attacks means that smaller FIs are equally susceptible.

Just as the meme stock phenomenon drove a wave of speculative trading because of social media, the "meme-ification of fraud" is fueling similar energy—but this time, it's leading individuals into illegal activities. Social media platforms like TikTok, YouTube Shorts and X (formerly Twitter) have amplified these fraudulent schemes, turning them into viral trends. Once a glitch is discovered, it quickly spreads online, attracting participants looking for quick, easy money. This phenomenon can create flash fraud and put FIs at risk. But it also directs significant attention toward smaller FIs, where defenses for both account opening and check fraud may be perceived as easier to bypass. Keep in mind that organized fraud rings require sophisticated mule rings to cash out effectively; usually with accounts spread across multiple FIs.

(Click the link in the title to continue reading.)

Enhancing Customer Protection: Encouraging the Use of a Trusted Contact Form - continued

How to Introduce the Trusted Contact Forum to Customers

When introducing the Trusted Contact Form to your customers, it's essential to frame it as an additional security measure that benefits them and their loved ones. Here are a few practical steps to encourage customers to complete the form:

1. Educate Customers During Routine Interactions: Whenever your team interacts with customers, whether during account openings, loan processing, or routine account reviews—bring up the importance of the Trusted Contact Form as part of their overall financial protection strategy. Explain how it helps in cases of potential fraud or identity theft.
2. Provide Clear and Simple Explanations: Many customers may not immediately understand the significance of a Trusted Contact Form. Provide them with easy-to-understand examples of when and how the bank might reach out to their trusted contact, emphasizing this person won't have direct access to their account but will only be informed if there is concern.
3. Make It Part of New Account Set-Up: Incorporate the Trusted Contact Form as a routine part of opening a new account. Many customers will be more open to completing this form when it's presented as a standard part of account security.
4. Use Digital Channels for Outreach: Send educational materials through email, mobile banking apps, and social media channels, encouraging customers to complete the Trusted Contact Form online or in person. Share real-life examples of how having a trusted contact in place has helped protect others from fraud.
5. Host Webinars or In-Person Events on Financial Safety: Organize informational sessions that discuss the rising threats of financial fraud and elder abuse, and offer guidance on how customers can protect themselves—including by completing the Trusted Contact Form.

A special thanks to CBM Preferred Partner SHAZAM for sharing this useful tool.