FRAUD PREVENTION FRIDAY

Friday, May 17, 2024

CBM Helps Community Banks Fight Fraud

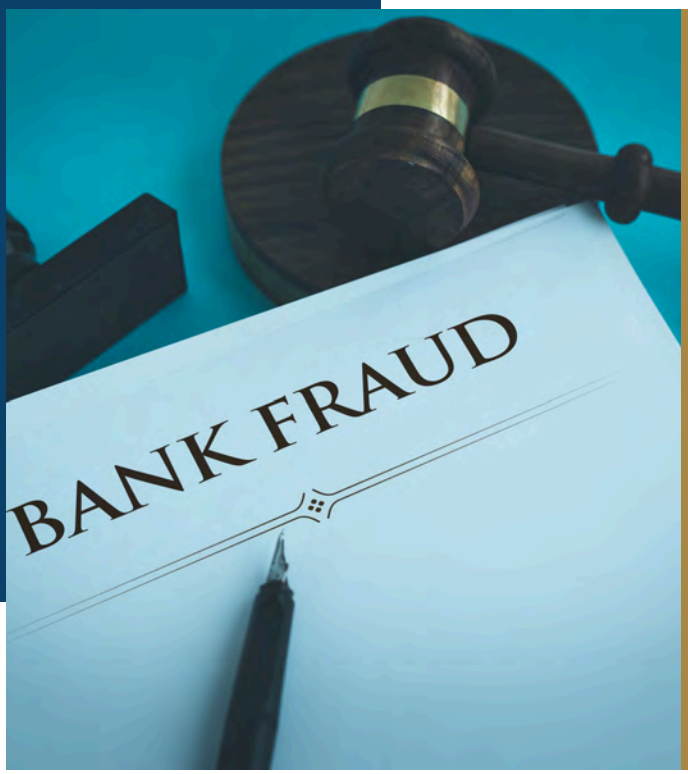
The fight against fraud is a constant battle, and community banks are often on the front lines. The CBM is proud to announce the launch of its brand-new **Fraud Prevention Friday** Newsletter. This bi-weekly resource will be delivered directly to your inbox, providing you with the latest tools and insights needed to safeguard your bank and your customers.

The CBM understands the unique challenges community banks face regarding fraud prevention. With limited resources, staying informed and proactive can be difficult. The Fraud Prevention Friday Newsletter bridges the gap, providing you with the knowledge and support you need to effectively combat fraud.

By working together, the CBM and community banks can create a stronger, more secure financial landscape for everyone.

Top News

- Agencies issue guide to assist community banks to develop and implement third-party risk management practices
- Cyber Threat Level: Elevated
- ICBA Fraud Task Force
- FinCEN Alert on Nationwide Surge in Mail Theft
- Harness AI's Large Language Models For Enhanced Anti-Fraud Defenses

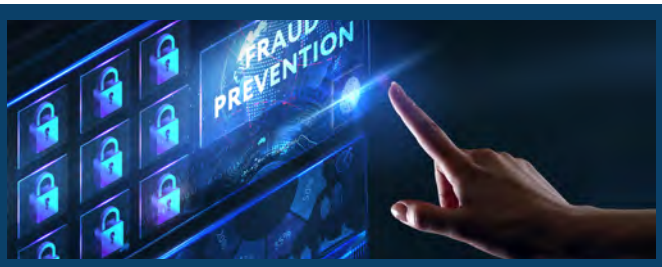


Cyber Threat Level: Elevated

Ongoing Scattered Spider activity targeting the Financial Services Sector warranted an elevated threat level. On May 13, 2024, the FBI reported it has had its eye on Scattered Spider since its origin in 2022, noting that it is particularly aggressive compared to other threat groups, threatening physical violence in some of its chats. Additionally, it has shown particular capabilities in stealing IT helpdesk identities in order to breach networks. Scattered Spider is reported to leverage advanced, targeted, mainly phone-based social engineering techniques. This includes tailored phishing domains, SIM swapping, phishing phone calls and targeted SMS. Implementation of additional cybersecurity measures may be warranted. Review procedures and stay vigilant.

Agencies issue guide to assist community banks to develop and implement third-party risk management practices

Community banks engage with third parties to help compete in and respond to an evolving financial services landscape. Third-party relationships present varied risks that community banks are expected to appropriately identify, assess, monitor, and control to ensure that their activities are performed in a safe and sound manner and in compliance with applicable laws and regulations. These laws and regulations include, but are not limited to, those designed to protect consumers and those addressing financial crimes.



ICBA Launches Fraud Task Force

The ICBA has recently launched a fraud task force focused on providing community bankers with effective tools and ammunition to help combat fraud. To begin, the focus of the task force is developing and providing information and guidance with:

1. Key forms and documents: introduction and ongoing library for members
2. Contacting regulators: how and when to engage
3. Counterfeit vs. altered checks: identification and implications of each
4. Fraud detection mechanisms: human and technology solutions
5. Front-line engagement with clients: information to share and communication options

The CBM has joined the task force to stay abreast of all issues and ensure all community bankers receive information and tools as soon as they are deployed. We are pleased to share Scott McQueen has joined the task force as well representing your interests.

Scott McQueen, 1st Vice President Risk Management, Southern Michigan Bank & Trust. Scott has 35 years in the banking industry with over 20 years dealing directly with fraud that includes check, ACH and wire fraud. Experience includes time spent in Risk Management. Compliance, BSA, Accounting and Operations.

U.S. Department of the Treasury Check Verification System

Be sure to share this useful resource with bankers to verify U.S. Treasury checks.

tcvs.fiscal.treasury.gov

FinCen Alert on Nationwide Surge in Mail Theft-related Check Fraud Schemes Targeting the U.S. Mail

In light of a nationwide surge in check fraud schemes targeting the U.S. Mail (hereinafter "mail theft-related check fraud"), the Financial Crimes Enforcement Network (FinCEN) is issuing this alert to financial institutions to be vigilant in identifying and reporting such activity. Mail theft-related check fraud generally pertains to the fraudulent negotiation of checks stolen from the U.S. Mail. Fraud, including check fraud, is the largest source of illicit proceeds in the United States and represents one of the most significant money laundering threats to the United States, as highlighted in the U.S. Department of the Treasury's most recent National Money Laundering Risk Assessment and National Strategy for Combatting Terrorist and other Illicit Financing. Fraud is also one of the anti-money laundering/countering the financing of terrorism (AML/CFT) National Priorities.

* This FinCEN alert is not new but the information continues to be relevant and used by many agencies combating fraud. For community banks especially, ensure the tips/guidance outlined on pages 4 & 5 are reviewed and processes and procedures are in place!

Harness AI's Large Language Models For Enhanced Anti-Fraud Defenses

The challenges facing financial institutions this year include the need to plug the growing educational gap and the ongoing shortage of qualified financial crime professionals to conduct effective client due diligence. With more work and fewer resources, firms must look to leverage cutting-edge technology to create a centralized financial crime ecosystem – including machine learning and artificial intelligence – to reduce the growing skills gap and, ultimately, mitigate the risk of further enforcement action over the coming 12 months." Rory Doyle, Head of Financial Crime Policy, Fenergo, January 2024.