FRAUD PREVENTION FRIDAY

Friday, December 6, 2024

CISA/ICBA Cyber Tabletop Exercise

December 11, 2024 | Noon EST | Webinar

This event for the 2024/2025 season will support and enhance the capabilities of community banks and the financial services sector in identifying, mitigating, responding to, and recovering from cyber incidents. This scenario is a cascading event with a cloud service provider cyber event and a regional disaster.

Exercise participants will be given the opportunity to explore the impacts of cyberattacks that compromise business operations and customer data and discuss their response plans, actions, and capabilities. While responding to the cyberattack a regional disaster impacts the community. Community bank technical staff, as well as senior leadership should participate as a team.

Registration

This three-hour cyber tabletop exercise will be conducted virtually in collaboration with CISA. Each member of your team should register individually, even if on the day of the event you will be in a shared location. Do not share log in information.

Registration questions? Call 800-422-7285 or email education@icba.org.

Top News

- CISA/ICBA Cyber Tabletop Exercise
- Physical Security Considerations to Protect Customers and Employees
- Protecting Your Community: Why Reporting to the IC3 is Crucial
- Insights from the Risk Fraud Forum: Current Payment Ecosystem Threats
- ICBA Releases Updated Check Fraud Guide

Physical Security Considerations to Protect Customers and Employees

The US Cybersecurity and Infrastructure Security Agency (CISA) just released its Venue Guide for Security Considerations. The document provides best practices to mitigate the threat of targeted violence and preparation for any potential incidents. The guide serves as a broad catalog to support safe and secure day-to-day operations, event management planning, and execution. The guide aims to help venue operators manage risk, enhance safety, protect assets, and create secure environments through effective security measures and best practices. The guide:

1. Helps venues evaluate security measures, complexity levels, costs, options, and threats mitigated by security measures. By balancing these factors, venues can create a secure environment for operators and guests.
2. Recommends broadly applicable considerations for evaluating security practices, such as assessing measures and improving physical security compliance to ensure staff and visitor safety.
3. Offers actionable guidance for prioritizing the most effective security practices and proactively reducing the risk of major threats.
4. Provides venue operators with a tailored menu of security options, allowing them to select the most suitable and effective measures for their venue's budget, size, location, and risk factors.

These guidelines help venue operators conduct risk assessment analysis to identify and address site-specific security vulnerabilities and proactively meet physical security expectations.

To learn more, visit Venue Guide for Security Considerations.

Protecting Your Community: Why Reporting to the IC3 is Crucial

As community bankers, one of your primary responsibilities is safeguarding your customers' financial security. In today's increasingly digital world, fraud has become a pervasive threat, affecting individuals and businesses alike. While educating customers about fraud prevention is vital, equally important is encouraging them to report fraud incidents to the appropriate authorities—namely, the Internet Crime Complaint Center (IC3).

Why Reporting Matters

1. **Creating a Record -** When your customers report fraud to the IC3, they create an official record of the incident. This documentation is often critical for investigations and for victims seeking reimbursement or legal recourse. It also demonstrates to regulators and law enforcement the scope and severity of cybercrime in your community.
2. **Helping Authorities Combat Crime -** Every report submitted to the IC3 contributes to a larger database that helps law enforcement agencies analyze and track fraudulent activity. Patterns and trends identified through these reports allow authorities to take action against criminals who might otherwise remain undetected.
3. **Protecting the Community -** Fraud is not an isolated incident—it often involves repeat offenders or criminal networks targeting multiple victims. When customers report fraud, they help protect others in the community by enabling proactive measures against these threats.
4. **Strengthening the Financial Sector -** Fraud erodes trust in financial institutions. By encouraging customers to report fraud, community banks demonstrate their commitment to transparency and security. This proactive approach reinforces confidence in your bank as a trusted partner in financial wellness.

How Community Banks Can Support Reporting

1. **Educate Your Customers** - Many individuals may not know what the IC3 is or why reporting fraud matters. Use newsletters, social media, and in-branch signage to inform customers about the IC3 and how to file a report. Emphasize that reporting is free, confidential, and can be done online.
2. **Simplify the Process** - Guide customers on how to report fraud to the IC3. Provide step-by-step instructions or host workshops to walk them through the process. You can even include the IC3 website link (www.ic3.gov) on your bank's fraud alerts or correspondence.
3. **Show Empathy** - Experiencing fraud can be stressful and emotional for your customers. Train your team to respond with understanding and support, guiding victims through the reporting process with compassion.
4. **Collaborate with Law Enforcement** - Establish relationships.

Insights From The CBM Risk Fraud Forum: Current Payment Ecosystem Threats

The CBM recently hosted a Risk Fraud Forum on Thursday, December 5, bringing together financial professionals and thought leaders to address the ever-evolving landscape of fraud and cybersecurity. This forum featured an engaging presentation from guest speaker Megan Monroe, Ph.D., an Intelligence and Cybercrime Senior Consultant at Visa Payment Ecosystem Risk and Control. Megan delivered a comprehensive analysis of current payment ecosystem threats and shared actionable insights to help community bankers stay one step ahead of fraudsters.

Community banks are often perceived as easier targets by fraudsters due to limited resources compared to larger institutions. However, staying informed and adopting proactive measures can make a significant difference. Megan's presentation reinforced the importance of vigilance and collaboration in securing the payment ecosystem.

We're excited to be able to share Megan's presentation from this week's forum to help strengthen your bank's fraud prevention strategies. Click the link in the title of this article to read her presentation.

We encourage all community bankers to assess their current fraud prevention measures in light of these evolving threats. If you missed the forum or would like more information, CBM members can access additional resources and session recordings on our website.

By staying informed and proactive, community banks can continue to protect their customers, build trust, and strengthen their role as pillars of financial security in their communities.

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

ICBA Releases Updated Check Fraud Guide - Engagement With Federal Bank Regulators

The Independent Community Bankers of America (ICBA) has advocated for the federal bank regulatory agencies to develop channels for banks to provide feedback related to problems resolving check fraud claims with other FDIC-insured depository institutions. This document offers suggestions on when to contact regulators, how to frame feedback, and where to direct your communication based on the experiences of peer community bankers.

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 only 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. Please follow internal bank operating procedures and policies and consult with legal counsel for specific questions.

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