FRAUD PREVENTION FRIDAY

Community Bankers of Michigan

Friday, January 10, 2024

Understanding The Processes, People and Technology Needed to Combat Check Fraud at Your Institution

During the ICBA Fraud Task Force meeting on December 10, 2024, Kerry Cantley, Vice President of Digital Banking Strategy at Mitek, delivered an insightful presentation. In her talk, Kerry focused on the critical topic of fraud detection and prevention in the digital banking landscape. She elaborated on various techniques for identifying fraud patterns, highlighting the importance of data analysis and behavioral insights in recognizing suspicious activities.

Kerry also shared strategies for effectively outsmarting fraudsters, discussing the evolving tactics employed by criminals and the necessity for financial institutions to stay one step ahead. Additionally, she addressed the multifaceted challenges organizations face in combating fraud, which encompasses processes, personnel, and technological obstacles. By providing a comprehensive overview of these issues, Kerry aimed to equip attendees with the knowledge and tools necessary to enhance their fraud prevention efforts and protect their institutions from evolving threats.

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

Top News

A Big Collapse of Trust: FrankonFraud Predictions for 2025

It was one for the history books. As expected, 2024 was "Fraud At Full Throttle" as fraudsters upped their attacks.

But it was the breakneck speed of everchanging scams that surprised us most. Just when we thought they could not get worse, they did. And when we felt that AI deepfakes were years away, they happened.

Scams ruin lives, tear families apart, and warp our sense of reality. But even worse, they poison our trust. Trust is the invisible glue that holds our society together. And here we are, watching it quickly fade away as scammers steal it from us.

Welcome to 2025, The Year of "A Great Collapse of Trust".

First, Let's Look Back At 2024 In Fraud – It Changed Everything

When we look back on 2024, one thing is clear. It was an explosive year of fraud that changed everything.

But it was these six things that defined the year.

In 2024, Glitch Culture Showed How Mob Mentality Has Taken Over Fraud

If 2021 was the era of FOMO for PPP funds, 2024 ushered in a new era of FOMO with people lining up for free money from ATMs compliments of "glitches." First, there was the Chase Glitch, then Fidelity and others.

Fraud Fighters realize that these glitches marked an ominous shift in first-party fraud. According to Mary Ann Miller, this happens when first-party fraud is unchecked.

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

CISA Urges All Organizations to Secure Cloud Environments

The Cybersecurity and Infrastructure Security Agency (CISA) issued Binding Operational Directive (BOD) 25-01, Implementing Secure Practices for Cloud Services to safeguard federal information and information systems. This Directive requires federal civilian agencies to identify specific cloud tenants, implement assessment tools, and align cloud environments to CISA's Secure Cloud Business Applications (SCuBA) secure configuration baselines.

Recent cybersecurity incidents highlight the significant risks posed by misconfigurations and weak security controls, which attackers can use to gain unauthorized access, exfiltrate data, or disrupt services. As part of CISA and the broad U.S. government's effort to move the federal civilian enterprise to a more defensible posture, this Directive will further reduce the attack surface of the federal government networks.

"Malicious threat actors are increasingly targeting cloud environments and evolving their tactics to gain initial cloud access. The actions required by agencies in this Directive are an important step in reducing risk to the federal civilian enterprise," said CISA Director Jen Easterly. "***While this Directive only applies to federal civilian agencies, the threat to cloud environments extends to every sector. We urge all organizations to adopt this guidance. When it comes to reducing cyber risk and ensuring resilience, we all have a role to play.***"

As federal civilian agencies implement this mandate, CISA will monitor and support agency adherence and provide additional resources as required. CISA is committed to using its cybersecurity authorities to gain greater visibility and drive timely risk reduction across federal civilian agencies.

The new Directive can be found by clicking the link in the title above. To learn more about CISA Directives, visit **Cybersecurity Directives** webpage.

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

FDIC Cyber Challenge: A Community Bank Cyber Exercise

The FDIC created Cyber Challenge: A Community Bank Cyber Exercise to encourage community financial institutions to discuss operational risk issues and the potential impact of information technology disruptions on common banking functions.

Cyber Challenge is a tool banks can use to help assess their readiness to confront operational risks and identify opportunities to strengthen their resilience.

The Challenge consists of different exercises presented using short video vignettes. Each exercise is designed to be completed in about an hour.

Each vignette represents a standalone operational scenario and has associated challenge questions to help prompt discussion. Participants can play the vignettes in any order they wish. They should discuss how they would address the event today and consider ways to mitigate risk in the future.

Institutions may use a free-flowing or facilitated discussion of the vignettes. You can click the link in the title for suggestions on organizing a facilitated discussion. These suggestions serve as a starting point. The format can be modified to fit the unique structure and character of each institution. For maximum effectiveness, the FDIC recommends members of senior management participate, along with key representatives from each of the financial institution's business lines.

(Click the heading link to read more.)

Phishing Scams Can Be Hard To Spot

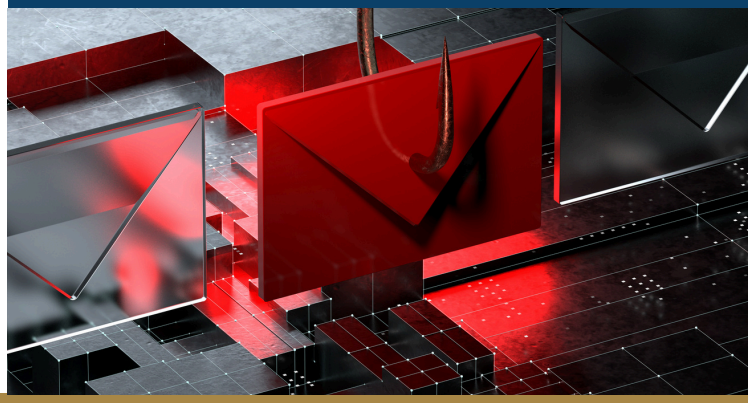
Scammers love a good disguise. One day they show up texting you about a delivery you missed, the next they say you need to sort an issue with your Netflix account. Here's how to avoid these phishing scams.

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. Maybe it's an unexpected email or text message pretending to be from a company you know or trust, like a utility company asking you to make a payment. Or maybe it's an unexpected party invitation that looks like it's from a friend or family member.

Don't click on links or download attachments in these messages. It might lead to a request for personal information, like your Social Security, credit card, or bank account number — and identity theft. Or, the link or attachment could download harmful malware onto your device.

How can you spot these scams? If you get an email or text message that asks you to click on a link or open an attachment, ask yourself: Do I have an account with the company or know the person who contacted me?

(Click the heading link to read more.)



Important Message From CBM Associate Partner QSI Regarding ATM Safety

ATM theft and fraud has been one of the many ways bad actors are working throughout Michigan and surrounding states. We've had member banks impacted. Don't assume this cannot happen in your area and ensure the appropriate individuals in your organization have all the latest information to keep your ATMs secure.

CBM Associate Partner QSI has recently sent messages regarding ATM jackpotting incidents, which are heating up, and ANY ATM CAN BE IMPACTED. EVERY MANUFACTURER'S ATM IS VULNERABLE TO MAN-IN-THE-MIDDLE ATTACKS. The information below is included in previous messages; however, several customers indicate many have not seen or read the updates.

There are two things QSI recommends banks do immediately if not already done:

- Contact your ATM driver/switch and have them TURN OFF OR DEACTIVATE FALL-BACK TO MAGNETIC STRIPE. Visa and MC have recommended this for a long time now.

- Use transport layer security (TLS 1.2) between the ATM and host where available or other communication security protocols like MAC flagging to encrypt the communications.

Both of these are done by the switch. QSI cannot do them. We cannot emphasize enough how critical this is.

Please take action immediately if you have not already done so. Forward this to the appropriate people in your organization if needed. Ensure these safety tips are followed whether you are a QSI customer or partner with anyone else.

Five Tips For Making Cybersecurity Part of Company Culture

For most places around the world, shaking your head usually means "no" and nodding means "yes", although this is not true everywhere. In Bulgaria, for example, the gestures are switched around: shaking your head means "yes", while nodding means "no." In France and Germany, the hand gesture for **"okay" is actually considered rude**. Understanding cultural differences like these can help travelers avoid confusion and potentially difficult situations.

Similarly, by embedding a strong cybersecurity culture across the organization, community financial institutions (CFIs) can help mitigate the difficulties associated with cybercrime.

Aside from the financial impact of a cyberattack — the global average cost of a data breach **is almost $4.9MM** — it can pose significant reputational, legal, and business continuity risks for CFIs. As such, prioritizing cybersecurity is a strategic necessity, crucial for gaining and maintaining customer trust, driving innovation, and meeting regulatory and privacy requirements.

Cyberattacks are becoming ever more sophisticated, as some of our own CFI customers discovered themselves when two employee email accounts were compromised, giving the fraudster a chance to trick the victims' coworkers into wiring substantial sums of money to fraudulent accounts overseas.

Having the right technology and digital infrastructure in place is no longer enough; fostering a cybersecurity culture throughout the organization is also key. A strong cybersecurity culture goes beyond prevention — it's about embedding security into everyday decisions at all levels of the institution.

CFIs should adopt a comprehensive, multifaceted cybersecurity strategy that includes advanced technology, robust governance, and regular employee training to build resilience and effectively respond to threats.

(Click the heading link to read more.)

Stay Ahead of Scammers in 2025

With scammers targeting our entire life savings with their schemes, we all need to be alert and know how to detect their latest tricks. Something as simple as talking about scams you know about is a great way to help you and your community stay protected. And being part of this solution doesn't require training or a lot of time!

The FTC has free materials and information on hundreds of different scams both in print and online. Here are a few ideas to help you become a fraud fighter.

- Learn more about what scammers say and do. Start at consumer.ftc.gov where you'll find articles, consumer alerts, and advice to help you spot and avoid scams.
- Check out resources in multiple languages. If you know people who prefer to get information in their native language, ftc.gov/languages has materials in more than a dozen languages.
- Get print materials to share with your community. Go to ftc.gov/BulkOrder and order free resources on a variety of consumer topics. Delivery is also free.
- Keep up with the latest. Sign up for FTC consumer alerts at ftc.gov/ConsumerAlerts to get email updates on recent scams, announcements, and advice.
- Share what you know. Have a conversation, leave FTC materials where people will see them, or post on social media. Are you part of a group? Consider using Pass It On or Pásalo presentations, complete with notes and supporting materials, to start a conversation about scams. All FTC content is in the public domain, which means there's no copyright or permission needed to use it.

Please remember the FTC wants to hear about scams in any language, even if you didn't lose money. Report in English at ReportFraud.ftc.gov — or in Spanish at ReporteFraude.ftc.gov. To report in other languages, call (877) 382-4357 and press 3 to speak to an interpreter in your preferred language.

Lessons Learned From Recent Fradulent Wires Targeting CFIs

During the last few weeks of 2024, the PCBB BID Daily Newsletter recapped some of their most popular articles of the year. We thought this was worth sharing again. Please read more below and follow the link in the heading for the full article.

Fraudsters impersonating known, trustworthy friends, family, and colleagues is nothing new. Yet, in PCBB's vast experience, this is the first case where the fraud is against the bank itself, not a bank's customer. Just this spring, two of PCBB's customers contacted our operations team with a similar story: an employee's account had been hacked, resulting in two fraudulent email requests for large wire transfers that were then processed.

To protect their privacy, we are simply referring to the institutions involved as "Bank A" and "Bank B." Curiously, both incidents occurred on the same day and the amounts of the wire transfers were also very similar — $950K and $2.95MM for Bank A, $950K and $2.35MM for Bank B.

We have spoken with an executive at Bank A as well as our own operations team about the incidents to gain insights about how each situation unfolded that can help our readers identify similar threats at their own institution and stop them before any harm is done.

When PCBB's operations team first received two large wire requests from each Bank A and Bank B via PCBB's Correspondent Bank Connection platform, PCBB made phone calls back to each bank. The CFI employees submitting the wires confirmed that the requests were made by them and ready for PCBB to process. Unbeknownst to the wire teams at Bank A and Bank B, the wire transfer requests that seemed to come from colleagues were actually being sent by fraud actors who had compromised their coworkers' accounts.