FRAUD PREVENTION FRIDAY

Community Bankers of Michigan

Friday, February 6, 2026

How Community Banks Can Fight AI-Driven Fraud

Source: ICBA

Ongoing advocacy efforts and artificial intelligence-powered fraud prevention tools have done wonders to help community banks fight fraud, but criminals are fanning the flames with AI of their own. They're using AI tools to generate phishing emails, create deepfake videos, clone voices, build synthetic identities and deploy bots to execute fraud schemes autonomously.

Fraud and scam operators have access to easy-to-use, low-cost tools that are readily available on the dark web. These tools make technologies that were recently considered cutting-edge, like real-time deepfake videos, accessible to even the most low-skill criminals. On the other end of the spectrum, highly sophisticated nation-state actors are using commercial, off-the-shelf tools to perpetrate large-scale fraud.

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

Top News

How QR Code Attacks Work and How to Protect Yourself

Source: First National Bank of Michigan

QR codes have become an integral part of our everyday life due to their simplicity. While they've been around for many years, their use exploded during the COVID-19 pandemic, when businesses turned to them for contactless menus, payments, and check-ins.

While QR codes are convenient, they also present significant risks. In the past few years, cybercriminals have increasingly turned to these codes as a tool to carry out scams.

QR code security risks

The main problem with QR codes is that users can't always verify the source before scanning. Since they can link to websites or other data, scammers can hide dangerous links or malware in them.

A term used to describe phishing attacks that involve QR codes is quishing.

Quishing attacks differ from traditional phishing scams in the way the malicious link is delivered. Instead of a standard text-based link in an email, attackers embed the link within a QR code. When a user scans the code, their device reads the embedded URL and directs them to the fraudulent website.

Help Net Security recently wrote about scammers who have used QR codes in physical letters to distribute Android malware.

Tampering with physical QR codes by replacing legitimate ones in public places—such as restaurant tables, parking meters, posters, or flyers—is a technique that has been growing in recent years.

(Click the heading link to read more.)

Widgets vs. Wisdom

Source: Mike Burke, Senior Financial Crimes Consultant, SHAZAM

I am often mind-boggled how community financial institutions sustain losses from fraud/scams relying on "widgets" instead of "wisdom".

I think we can all agree that knowledge is power.

I have conducted hundreds of "Townhall Meetings" addressing fraud for community financial institutions nationwide…and it works.

What is a "Townhall Meeting"?

A townhall meeting is set up by a local community financial institution to engage their community in identifying and helping their clients/members not to fall victim to fraud…. better yet…trusting their community financial institution to be the "trusted partner" to help their community not fall victim to scams and fraud.

Unfortunately, this is not a one-and-done.

The town hall meeting should be the kickoff for a fraud campaign.

Prior to the town hall meeting, free…I will repeat…. FREE…brochures and pamphlets from the Federal Trade Commission (FTC) are available as leave-behinds at the town hall meetings. These leave-behinds can be ordered from https://lnkd.in/gUJeUVyU. Delivery usually takes a few weeks, so plan accordingly. Following this up with weekly, not monthly, weekly or bi-weekly social media updates relating to fraud.

(Click the heading link to order FTC resources.)

How Social Media is Fueling Check Fraud

Source: ProSight

Many Americans still write checks for at least some transactions—a preference that leaves consumers and financial institutions exposed to mail theft and check washing.

Today's mix of paper checks and digital payments requires fraud defenses across banking touchpoints. And while "low tech" check writing persists, a near ubiquity of smartphones (and other connected devices) and constant online engagement gives bad actors more ways to exploit unguarded data and mine social media and other accounts to facilitate check fraud.

For instance, fraudsters might intercept details found through social media "oversharing" or when unwary consumers transact on commercial sites without precautions, especially via pop-ups.

Some fraudsters prey on human psychology with friendly or romantic manipulation that may begin as casual messaging. Some snare victims with illegitimate offers. "Financial criminals have been using social engineering in various ways for many years whether it's personally identifiable information (PII) or flat-out seeking bank account information," said Staci Shatsoff, assistant vice president of payments improvement at Federal Reserve Financial Services. "And social media is a great outlet for this access."

The fraudster then leverages that intelligence to rewrite stolen checks, and more sophisticated abusers use advanced chemicals and ink that often evade suspicion. More ambitious criminals may collect enough PII to slide into a legitimate checking account as an imposter, often fooling financial institutions.

(Click the heading link to read more.)

Blind Spots in Your Cyber Insurance Coverage Could Cost You

Source: PCBB BID Daily Newsletter

As a leader at your CFI, you'll want to review your risk, consider your choice of insurer, and review your coverage to make sure you're protected in the spots where you want and need protection.

For many banks, the biggest driver of a gap between cyber incident costs and insurance payout is that total losses end up higher than the policy's limits or sub-limits. Other common factors include: certain types of costs not being covered under the policy, expenses incurred before the carrier was notified or without the carrier's consent, or the bank not meeting the cybersecurity controls and other conditions the policy required.

The most common cyber crimes exploit human trust and weak digital controls. For companies with less than $2B in revenue, ransomware is the most likely cyber threat. It accounts for 64% of cyber losses. AI-powered social engineering to create deepfakes and hyper-personalized phishing, as well as advanced impersonation scams, pig butchering, fraud, and traditional data breaches, are also worries for CFIs.

The longer a CFI's systems are down in the wake of an attack, the more an attack is likely to cost in direct damage, lost work time, limited account access, and damaged customer trust.

It's vital that CFIs pick the right insurer. Choose an insurance company that specializes in cyber coverage for financial institutions and has experience working with CFIs.

(Click the heading link to read more.)