FRAUD PREVENTION FRIDAY

Community Bankers of Michigan

Friday, April 17, 2026

Helping Customers Pause to Prevent Scams

Source: Community Bankers of Michigan

Scams increasingly rely on urgency and emotion, making front-line bank staff the last line of defense. To support that moment, we developed a practical training program that helps employees spot scam signals and confidently encourage customers to pause before withdrawing or wiring funds.

The training focuses on real-world conversations, teaching staff how to recognize red flags, ask respectful questions, and slow a transaction without damaging trust. The goal is not confrontation, but protection.

Included is a manager coaching guide that clarifies leaders' roles in building these skills over time. Managers learn how to observe behaviors, coach effectively, and reinforce consistent, customer-centered scam prevention across the team.

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

Top News

Cryptocurrency and AI Scams Bilk Americans of Billions

Source: FBI

FBI releases annual internet crime complaint report

The FBI's 2025 Internet Crime Report shows cyber-enabled crimes defrauded Americans of nearly $21 billion, with cryptocurrency and artificial intelligence-related complaints among the costliest.

The Internet Crime Complaint Center (IC3) received 1,008,597 total complaints, an increase from 859,532 in 2024. Phishing/spoofing, extortion, and investment schemes were the most frequently reported complaints. Americans over 60 reported approximately $7.7 billion in losses, up 37% from 2024.

The IC3 received approximately 453,000 cyber-enabled fraud complaints, with reported losses exceeding $17.7 billion. Investment fraud remains the primary driver, accounting for nearly 49% of all scam-related losses.

Americans who submitted complaints involving cryptocurrency reported the highest losses, with 181,565 complaints totaling more than $11 billion. In 2024, the FBI launched Operation Level Up, a proactive initiative to identify and notify people who are currently falling victim to cryptocurrency investment fraud. Since its inception, the initiative has surpassed 8,000 total victims notified and reduced losses by more than $500 million. In 2026, the FBI launched Operation Winter SHIELD, highlighting concrete steps organizations can take to bolster their digital security.

(Click the heading link to read more.)

2026 Fraud Insights U.S. Payments Edition

Source: NICE Actimize

Fraud prevention has become a critical priority for community banks, and social media offers a powerful way to connect with customers through timely, consistent education. A successful fraud prevention social media campaign combines clear messaging, practical tips, and visual reinforcement, an approach outlined in Cross Financial's Fraud Prevention Communication Ideas 2026.

The Cross Financial framework provides a structured 12-week social media campaign designed specifically for community banks. Each weekly post focuses on a core aspect of fraud awareness, including recognition of common scams, understanding fraudster tactics, and knowing how to respond when suspicious activity occurs. Posts follow a simple, repeatable format: headline, short explanation, single actionable tip, and suggested visuals, making the content easy for customers to understand and easy for banks to deploy.

Key campaign topics include phishing and smishing scams, fake urgency messages, caller ID spoofing, protection of personal information, and steps to take if fraud is suspected. By addressing these risks individually over time, the campaign reinforces learning and avoids overwhelming customers with too much information at once. Consistent themes such as "pause and verify," "never share passwords or verification codes," and "contact your bank directly" help consumers build safer habits.

(Click the heading link to read more.)

ACH Fraud and Nacha's New Rules: Why Now Is The Time To Act

Source: ProSight

The scale and sophistication of consumer scams in today's digital economy are staggering. Globally, losses related to these scams reached $43.6 billion in 2023, with business email compromise (BEC)—a type of social engineering attack that exploits trust in email communications—accounting for $6.7 billion in losses alone.

Despite this risk, the Association of Financial Professionals reported in 2024 that less than 60% of institutions have developed procedures to safeguard against BEC. More than half of those have never tested their effectiveness. When fraud detection is siloed, resulting in overwhelming volumes of false-positive alerts, financial institutions are unable to respond effectively, leaving them open to real threats.

An attempt to solve the problem

The 2026 rules from the National Automated Clearing House Association (Nacha) are a direct response to the evolving landscape of ACH fraud. The Nacha ACH Network has reported 11 consecutive years of growth, adding **$1 trillion in transaction volume each year**— a testament to the critical role ACH payments play in commerce. But as the network expands, so do the opportunities for fraudsters, who are relentlessly following the money.

The new rules are designed to address the challenges of detecting fraudulent transactions authorized through social engineering and other attacks that target ACH payments. The updates require both receiving depository financial institutions (RDFIs) and originating depository financial institutions (ODFIs) to rigorously assess both sides of an ACH payment, analyzing all 17 monetary Standard Entry Class (SEC) codes.

(Click the heading link to read more.)

The Hidden Value of Friction

Source: BioCatch

Our industry has long recognized "friction" as one of the dirtiest words in banking. Its connotation suggests a thick fog of failed logins, dropped online sessions, incomplete transactions, lost revenue, reduced engagement, plummeting new account conversions, and an overwhelming sense of dysfunction. We treat friction as a measure of failure, a KPI of unrealized potential, and a brand of attrition.

But is it always? Does it have to be? Are we making this too binary? Can we not find a glimmer of success in the failure to complete a digital banking task?

I'd challenge us to push back on the stereotype of friction as some cardinal sin. If we can precisely apply targeted friction (spoiler: We can), that is a science we ought to embrace.

I always like to tell my colleagues and clients that fraud operations isn't a cost center. It's something more akin to a place where the nuanced accounting term "contra liability" emerges. Fraud in this light isn't about losses. It's the art of the successful prevention of those losses. And this is where friction is a gift.

So, what if there were benefits to friction? What if we could demonstrate how friction adds value, helps to retain customers, and increases brand affinity?

A recent Notre Dame study found those institutions most successful at mitigating fraud were the same institutions whose customers felt most confident in their bank as the custodian of their hard-earned money.

(Click the heading link to read more.)