FRAUD PREVENTION FRIDAY

Community Bankers of Michigan

Friday, August 7, 2026

How Community Bankers Can Join the Fight to #StandAgaintScammers

Source: ICBA

Fraud and scams continue to be one of the greatest threats facing consumers today. Whether it's a cryptocurrency investment scam, fake job opportunity, romance scam, family emergency scam, or business email compromise, fraudsters are constantly evolving their tactics to deceive consumers.

While community banks work tirelessly to protect their customers through education, fraud prevention tools, and vigilant frontline staff trained to identify potential scams before money leaves an account, the reality is that anyone can become a victim of a scam—regardless of age, education, or financial experience.

Because scams continue to evolve, customer awareness remains one of the strongest defenses.

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

Top News

- How Community Bankers Can Join the Fight to #StandAgaintScammers
- Talk to Your Friends and Family to Fight Fraud
- FinCEN Issues Alert on Fraud Schemes Targeting Federal Student Aid
- Where AI Fits in a Mature Fraud Program
- Cyber-fraud Integration for the New Age of Risk - A Worldwide Study

Talk to Your Friends and Family to Fight Fraud

Source: Federal Trade Commission Consumer Advice

One of the best ways to fight fraud is to talk about it. When you know scammers' tactics, they're easier to spot and avoid. The FTC has some facts about fraud to help you start the conversation.

- Imposters are the #1 scam the FTC sees. Scammers send texts pretending to be a business like your bank, saying you need to verify a (fake) transaction to "protect" (but really: steal) your money. Or they're a "government organization" like a state toll agency, telling you to pay (fake) tolls. To confirm it's legit, check with the real organization, but use a phone number or website you know is real — not the info from the call or message.
- People report losing lots of money to investment scams. Scammers know that promising big returns on investments might get you to open your wallet. But do some research to avoid these scams. Many investment scams start with unlicensed people or unregistered firms, so use the free search tool on Investor.gov to check out anyone recommending or selling investments.
- Scammers love to text. People tell the FTC it's the main way scammers got in touch — thanks mainly to toll scams. But it's far from the only way. They're still calling (a lot) and reaching many people through social media. The takeaway? Scammers are everywhere we are, always finding ways to get our attention. So, watch for signs of a scam and check it out if in doubt.
- Scammers say you have to pay a specific way. People report recent losses through bank transfers and cryptocurrency, but scammers also like demanding payment by wire transfer, payment app, and gift card. If anyone ever says the ONLY way to pay is any one of these, get your scam antennae up.

(Click the heading link to read more.)

FinCEN Issues Alert on Fraud Schemes Targeting Federal Student Aid

Source: The U.S. Department of Treasury - FinCEN

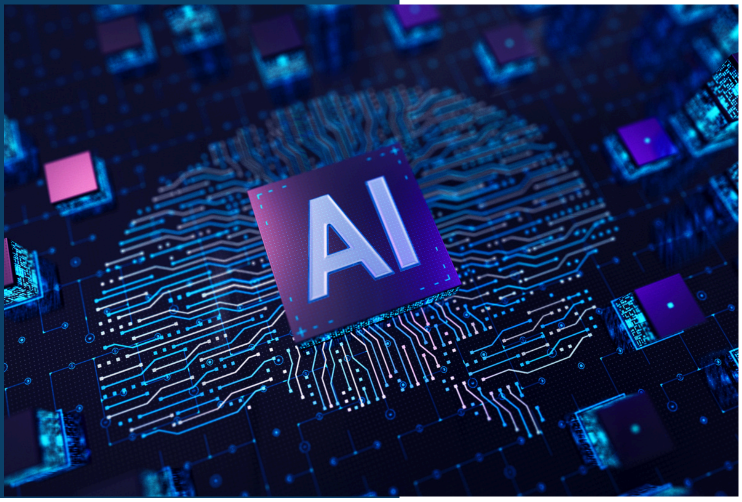
The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued an Alert urging financial institutions to detect, prevent, and report suspicious activity connected to fraud schemes targeting student aid programs administered by the Federal government. Today's action is the latest in Treasury's efforts, led by President Trump and Vice President Vance, to eliminate government benefits fraud.

"Every dollar stolen from Federal student aid is a dollar taken from taxpayers and deserving students," said Secretary of the Treasury Scott Bessent. "The Trump Administration will not tolerate criminals who exploit government programs for personal gain. Treasury is working with financial institutions and law enforcement to identify these fraud schemes, recover stolen funds, and hold those responsible accountable."

Fraud rings use stolen and fraudulent identities, as well as other tactics, to enroll in educational institutions and unlawfully acquire funds from Federal student aid programs. The schemes not only result in losses to Federal student aid programs, but in some cases, real students face difficulties enrolling in classes because of the number of fraudulently enrolled "students."

Fraudsters Steal Personally Identifiable Information to Create "Ghost Students"

(Click the heading link to read more.)



Where AI Fits in a Mature Fraud Program

Source: ProSight

The strongest fraud programs use AI to sharpen detection, reduce friction, and uncover connections across accounts, devices, identities, and transactions—while keeping people accountable for consequential decisions. That combination of automation, layered controls, governance, and human judgment is becoming increasingly important as fraudsters use the same technology to make attacks more convincing, easier to scale, and increasingly organized like business operations.

In a ProSight Banking Strategies podcast discussion, Bobbie Paul, managing director for fraud at Huron, described this approach as "accountable augmentation." Banks have access to strong data, behavioral analytics, fraud intelligence, and established controls, she explained, but they also must ensure that AI-supported decisions remain accurate, explainable, and subject to meaningful challenge.

Paul emphasized several priorities for putting that approach into practice:

Build layers rather than relying on one model. Effective fraud programs combine behavioral analytics, anomaly detection, entity resolution, link analysis, supervised machine learning, unsupervised pattern detection, and other controls. Graph and network analytics can be especially valuable because fraud often connects identities, devices, accounts, and transactions that appear unrelated when viewed separately.

Institutions should deploy those capabilities according to risk rather than applying every control everywhere.

(Click the heading link to read more.)

Cyber-fraud Integration for the New Age of Risk - A Worldwide Study

Source: Datos Insights

Criminal teams operating with unprecedented scale, agility and sophistication are levying attacks against consumers and financial institutions (FIs) with increasing effectiveness and speed. Payments fraud continues to increase across the globe, shadowing consumer growth in using real-time payment services. Card fraud continues to rise, posing a significant business challenge for issuers, processors and merchants worldwide.

FI fraud and risk leaders face daunting challenges now and into the foreseeable future. In the age of cyber risk, indicators of potential fraud often present first through cybersecurity data anomalies. Many card issuers and processors are pursuing cyber-fraud integration efforts to harness the combined data and talents of their fraud and cybersecurity teams. Implemented in different models, cyber-fraud integration has proven difficult to deliver the desired outcomes for businesses. This report examines the challenges and opportunities associated with cyber-fraud integration programs through a worldwide study of 100 FIs, providing strategic insights and recommendations to card fraud, retail payments fraud, CISOs and risk leaders.

Key considerations

Who this impacts most: Enterprise fraud executives and CISOs serving FIs, card issuers and card processors serving consumers in the market will find this analysis critical to their integration strategies, as will emerging executive titles, such as chief...

(Click the heading link to read more.)