FRAUD PREVENTION FRIDAY

CBM
Community Bankers of Michigan

FRIDAY, OCTOBER 31, 2025

Keeping Up With Instant Payments Fraud

Source: Independent Banker

With instant payments becoming more mainstream, there are more opportunities for fraud. Reports indicate that instant payment fraud has been limited so far, but projected growth in these payments could increase the volume of authorized push payment (APP) scams. Luckily, in the past year, the industry has shifted toward proactive fraud prevention, and FedNow and The Clearing House's RTP network have enhanced their fraud-related rules and tools.

For FedNow, the Federal Reserve has set a maximum transaction amount at the network level, capped the amount a correspondent can send on behalf of others, and allowed institutions to set lower limits based on their own risk policies. Those same institutions can block transactions to or from suspicious accounts and set limits on how much money customers can send and the size of each transaction, based on the type of customer. Participants must report suspected fraud promptly to help contain threats, and banks can request the return of funds from transactions flagged as fraudulent.

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

TOP NEWS

- Keeping Up With Instant Payments Fraud
- DIFS and MDHHS Share Tips to Help Seniors Avoid Scams During Medicare Open Enrollment Period
- What Is First-Party Fraud, And Why Is It Concerning?
- Is Microsoft Copilot Exposing Your Data?
- Fraud is Evolving. Here's What Banks Need to Watch and Where to Find Help

DIFS and MDHHS Share Tips to Help Seniors Avoid Scams During Medicare Open Enrollment Period

Source: Department of Insurance and Financial Services (DIFS)

The Michigan Department of Insurance and Financial Services (DIFS) and the Michigan Department of Health and Human Services (MDHHS) are alerting Michigan seniors about scams and high-pressure sales tactics during the annual Medicare Open Enrollment period, which runs from October 15, 2025, through December 7, 2025.

“The Medicare Open Enrollment period is a time for Michigan seniors to make important decisions about their health insurance and prescription drug coverage,” said DIFS Director Anita Fox. “Unfortunately, it also provides the opportunity for criminals and scammers to try to take advantage of seniors to steal their money or personal information. Current enrollees and those enrolling in Medicare for the first time can protect themselves by never giving out any information to anyone who contacts them over the phone, online, or in-person.”

"We want to make sure that Michigan residents get access to the health care coverage they need without being taken advantage of by scammers," said MDHHS Director Elizabeth Hertel. "We also want to remind Michigan families of a new resource, the MI Options call center, which can connect people with free counseling to help them navigate Medicare plan options or enrollment by calling 800-803-7174."

To help protect Michiganders from Medicare scams and high-pressure sales efforts, DIFS and MDHHS have some helpful tips:

(Click the heading link to read more.)

What Is First-Party Fraud, And Why Is It Concerning?

Source: PCBB BID Daily Newsletter

The same frame of mind that drives the protagonists in heist films can also apply to a different type of financial crime: first-party fraud. This brand of fraud occurs when customers themselves intentionally deceive their financial institution for monetary gain.

First-party fraud is now the leading type of fraud across the world. One-third (36%) of all reported fraud in 2024, up from 15% the year before, according to LexisNexis Risk Solutions. This year, Datos Insights expects **losses from first-party fraud to reach $3.9B** before climbing to $4.8B by 2028.

"First-party fraud has always been around and in the last couple of years, I'm hearing bankers talk a lot more about frustration over the fact that their own customers are committing fraud, which makes it a lot more difficult to find and to mitigate," Datos Insights' **Jim Mortensen says**. "You always concern yourself with third-party fraudsters who were attacking both you and your customer, and now you've got your customer attacking you." Essentially, the rise of first-party fraud erodes trust between a customer and their financial institution.

What are the types of first-party fraud?

- Transactional fraud. Such fraud occurs when a customer disputes a purchase on their credit or debit card that they actually made. They might also allege that goods from an online purchase were never delivered, hoping for a chargeback to their account. Annual losses from such fraud are roughly $50B, according to Mastercard.

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

Is Microsoft Copilot Exposing Your Data?

Source: FinCyberTech

Without the right Data Loss Prevention (DLP) configuration and sensitivity labeling policies, sensitive data is just one query away from exposure.

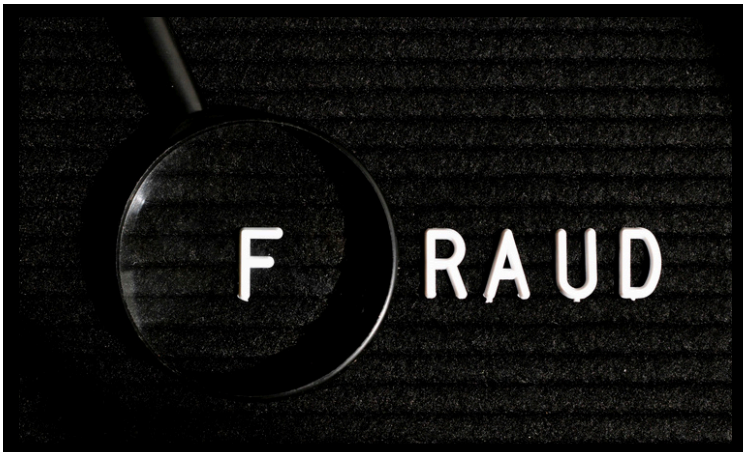
Financial institutions are rapidly adopting Microsoft Copilot Enterprise Edition while moving away from the use of consumer-grade generative AI platforms such as ChatGPT. The enterprise edition offers governance, compliance alignment, and built-in safeguards that reduce the likelihood of sensitive customer or financial data being exposed outside the organization.

Previously, when employees used publicly available AI platforms on their own, organizations had no control over where queries were stored, how they were processed, or whether sensitive data was retained or exposed. This created serious regulatory blind spots and heightened the risk of noncompliance with financial regulations. By standardizing enterprise-grade AI, institutions can harness the productivity benefits of generative AI while maintaining compliance, security, and control.

The Hidden Risk: Overexposure of Internal Data

As employees begin using Copilot to summarize documents, draft communications, generate code, and retrieve information, many institutions are discovering that the tool has broader access than expected. Because Copilot is deeply integrated with Office 365, SharePoint, OneDrive, Teams, and network file shares, it may surface information from sources that employees can technically access but were never expected to interact with.

(Click the heading link to read more.)



Fraud is Evolving. Here's What Banks Need to Watch and Where to Find Help

Source: BAI

Fraud threats aren't standing still—and neither can banks. Check fraud is back. Card-not-present fraud is rising. Synthetic identities are harder to spot. And fraudsters are better organized than ever. As Jason Bartolacci, director of ProSight's Fraud Alert Network, put it recently, the threat landscape is expanding. Institutions can't go it alone and neither can any individual banking department.

The good news: There are proven ways to push back. From his work leading ProSight's Fraud Alert Network and engaging with peers across the industry, Bartolacci highlights five urgent trends—and the practical steps banks can take to fight back:

- Don't underestimate old scams. Check fraud is up 385% since the pandemic. Criminals are raiding mailrooms and using brake fluid to wash checks clean. In 2024, only 22% of affected organizations recovered at least 75% of stolen funds—down from 41% the year before. Even the U.S. Treasury, which still issues billions in paper checks, is feeling the pressure.
- Breached data is fueling synthetic IDs. In 2024 alone, six "mega-breaches" triggered 1.7 billion victim notices. Criminals are combining real data with fake details to create new identities that sail past fraud filters. With no victim to report, alerts are delayed. Meanwhile, card-not-present fraud continues its surge, with global losses projected at $400 billion over the next decade.

(Click the heading link to read more.)