FRAUD PREVENTION FRIDAY

Community Bankers of Michigan

Friday, May 1, 2026

FDIC Warns of 'Ramp and Dump' Schemes

Source: FDIC Office of Inspector General

The FDIC OIG is warning investors and the public about a type of investment fraud scheme known as "Ramp and Dump."

In a "Ramp and Dump" scheme (which is a type of Pump and Dump scheme), Chinese or other micro/small-cap non-U.S. companies, typically valued at $15 million or less, with an individual share price of $4-6 at the Initial Public Offering (IPO) will obtain a listing on the NASDAQ and go public, while the bad actors are allocated millions of pre-IPO shares at little to no cost to themselves.

Leading up to an IPO event, bad actors will solicit investors through WhatsApp group chats by making false claims about the value and instructing the victims to purchase shares on the day of an IPO at a specific time.

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

Top News

The Rising Tide of Debit Card Fraud

Source: Lasco

Simply put, Debit Card Fraud is the unauthorized use of a person's debit card. It can happen through the physical theft of a card, or by stealing card information. Stealing information can be accomplished online, by deceiving someone into giving up their card information, or with "skimming" devices placed on ATMs, gas pumps, or other self-serve equipment.

For consumers, the consequences are obvious—a bad actor can steal money directly from an account. For banking institutions, Debit Card Fraud can also erode trust. It's important to ensure that measures are taken by both the customer and the bank to limit fraudulent activity.

Card Fraud is the Costliest Fraud Category for Community Banks

Debit card fraud has surged to become one of the most pressing operational and financial threats facing community banks today. As digital payments proliferate and fraudsters adopt increasingly sophisticated tactics, smaller financial institutions, often operating with leaner technology budgets, are experiencing disproportionate exposure to losses and customer disruption.

According to the 2025 Conference of State Bank Supervisors (CSBS) Annual Survey, card fraud accounted for 59% of all reported fraud cases and 39% of total fraud losses at community banks. "Smart Ways Community Banks Can Address Card Fraud", ICBA.

(Click the heading link to read more.)

2026 Anti-Fraud Technology Benchmarking Report

Source: Association of Certified Fraud Examiners

The utilization of technology by both organizations and the fraudsters who target them has become one of the defining characteristics of the anti-fraud profession in recent years. Anti-fraud professionals and organizational leaders must take steps to continually evaluate both long-standing and emerging technologies. The capabilities need to consider their potential impact as components of a comprehensive anti-fraud program, as well as a source of threats to defend against.

To help organizations and anti-fraud professionals in this endeavor, the ACFE and SAS have partnered to conduct a series of studies on the use of technology in anti-fraud programs by organizations throughout the world. This benchmarking report represents the fourth edition of this series, and for the first time incorporates information about how fraudsters are using technology to further their schemes. We have also expanded the breadth of technologies explored in the report, including more generative artificial intelligence (AI) tools and their applications, quantum computing, automation, and cloud computing. The findings of this study are valuable for anti-fraud professionals, the organizations that employ them, and others in the industry. The report provides insights into opportunities and vulnerabilities presented by technologies, benchmarking of anti-fraud programs' technology, and how to preparing for future technological developments with fraud resilience at the forefront.

(Click the heading link to read more.)

With People Losing Big to Investment Scams, Learn How to Spot and Avoid Them

Source: Federal Trade Commission Consumer Advice

You might be interested in making money through investments. Who isn't? So offers that promise big returns might draw your attention…and scammers know this. They use those promises and clever schemes to lure you in and, unfortunately, people are losing big money on investment scams. In fact, FTC data shows reports of more than $7.9 billion in losses to investment scams, with a median individual loss of more than $10,000 in 2025. Do you know how to spot and avoid investment scams?

Scammers might reach you through social media, WhatsApp, or through online ads, promising you'll make a lot of money quickly. These messages might also come from a friend or love interest offering you "coaching" to learn how to make a fortune in stocks, forex, or cryptocurrency. After you invest, they'll often say your investments are doing well, maybe even showing fake "proof" that you're making money. The reality? The investment isn't real and you end up losing all your money.

To avoid an investment scam:

- **Remember that investments always involve risk**. If anyone plays down the risk of an investment or acts like risk disclosures are just a formality you don't need to worry about, keep your money. Those are scammers who want you to think their opportunity is risk-free when it's not.
- **Check out the reputation of the investment company, its officials, and its promoters**. Search online with their name plus words like "review," "scam," or "complaint." Go through several pages of search results.

(Click the heading link to read more.)

AI Fraud is Rising: 2026 Industry Pulse Highlights

Source: Veriff

Online fraud is transforming right before our eyes. Criminals now have access to powerful artificial intelligence tools, making their attacks faster, cheaper, and far more convincing. But technology also gives us the exact tools we need to fight back and secure our platforms.

Veriff recently released the Fraud Industry Pulse Report 2026, surveying nearly 1,200 fraud and compliance decision-makers worldwide. The findings paint a clear picture of a rapidly changing security landscape. The data shows exactly what fraud professionals face daily and how they plan to adapt.

This post breaks down the most critical takeaways from the report. We will explore the surging threat of AI-driven fraud, the ways companies use AI for prevention, and the massive shift toward robust identity verification. You will also learn about the top challenges organizations face and why your executive team needs to pay close attention.

The growing threat of AI-driven fraud

Fraud is not just increasing; it is evolving. Almost 74% of surveyed professionals reported a general increase in online fraud over the past year. This growth brings severe financial consequences, with 85% of businesses suffering negative financial impacts directly linked to fraudulent activity.

(Click the heading link to read more.)