FRAUD PREVENTION FRIDAY

Community Bankers of Michigan

Friday, March 6, 2026

Treasury Announces Public-Private Initiative to Strengthen Cybersecurity and Risk Management for AI

Source: U.S. Department of the Treasury

In support of the President's AI Action Plan, the U.S. Department of the Treasury recently announced the conclusion of a major public-private initiative to strengthen cybersecurity and risk management for artificial intelligence (AI) in the financial services sector. Over the course of February, Treasury will release a series of six resources developed in partnership with industry and federal and state regulatory partners to enable secure and resilient AI across the U.S. financial system.

"As this Administration has made clear, it is imperative that the United States take the lead on developing innovative uses for artificial intelligence, and nowhere is that more important than in the financial sector," said Secretary of the Treasury Scott Bessent.

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

Top News

Increase in Malware-Enabled ATM Jackpotting Incidents Across United States

Source: Federal Bureau of Investigation

The Federal Bureau of Investigation (FBI) is releasing this FLASH to disseminate indicators of compromise (IOCs) and technical details associated with malware enabled ATM jackpotting. Threat actors exploit physical and software vulnerabilities in ATMs and deploy malware to dispense cash without a legitimate transaction. The FBI has observed an increase in ATM jackpotting incidents across the United States. Out of 1,900 ATM jackpotting incidents reported since 2020, over 700 of them with more than $20 million in losses occurred in 2025 alone. This FLASH is being provided to encourage organizations to implement the recommended mitigation steps and to outline the information requested from the public.

Threat actors are deploying ATM jackpotting malware, including the Ploutus family malware, to infect ATMs and force them to dispense cash. Ploutus malware exploits the eXtensions for Financial Services (XFS), the layer of software that instructs an ATM what to physically do. When a legitimate transaction occurs, the ATM application sends instructions through XFS for bank authorization. If a threat actor can issue their own commands to XFS, they can bypass bank authorization entirely and instruct the ATM to dispense cash on demand. As a result, Ploutus allows threat actors to force an ATM to dispense cash without using a bank card, customer account, or bank authorization. Once Ploutus is installed on an ATM, it gives threat actors direct control over the machine, allowing them to trigger cash withdrawals. Ploutus attacks the ATM itself rather than customer accounts, enabling fast cash-out operations that can occur in minutes and are often difficult to detect until after the money is withdrawn.

(Click the heading link to read more.)

As Threats Converge, Banks Rethink Fraud-Cyber Cooperation

Source: ProSight

Criminals today move seamlessly across digital channels. Banks, for the most part, still have gaps. That's due in large part to fragmented technology.

As fraud and cyber threats increasingly overlap, many financial institutions are discovering that their biggest vulnerability is not detection, but internal coordination. Fraud teams, cybersecurity teams, and frontline staff often investigate the same incident separately, using different systems, timelines, and definitions of success. This disconnect can frustrate customers, obscure patterns, and slow response. Plus, the disparate effort can add to operational costs.

That challenge was a recurring theme during a panel discussion at ProSight's recent Annual Risk, Compliance, and Fraud Virtual Conference. Industry leaders emphasized at the event that banks and credit unions are incentivized to rethink how fraud and cyber teams can share intelligence and manage incidents in parallel with one another.

Bad actors "don't look at themselves as cyber or fraud or physical security," said Lawrence Zelvin, executive vice president and head of the financial crimes unit at BMO Financial Group. "They look at themselves as opportunists. They look at, here's what I want to do, and here's what it's going to take to get there."

Siloed responses can mean multiple teams unknowingly working the same event.

(Click the heading link to read more.)

2026 State of Document Fraud

Source: Inscribe

Fraudsters have always sought to exploit the gap between what a document claims and what is actually true.

In the 1920s, Victor Lustig used fake documents to pose as a government official and convince scrap metal dealers to purchase the Eiffel Tower (twice). What's different 100 years later is the scale and speed at which that exploitation can happen.

Today, generative AI can help produce a realistic pay stub in seconds. Template marketplaces sell editable bank statements for under ten dollars. A fraudster with no technical skills can purchase, customize, and submit convincing documentation without ever touching Photoshop.

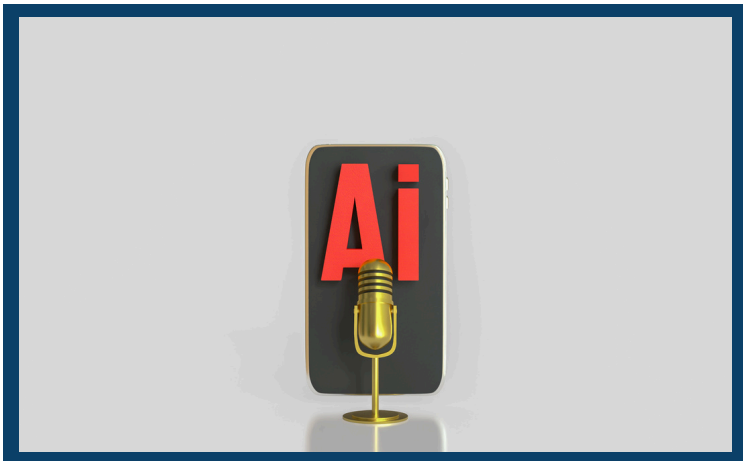
And it is working. Inscribe flagged approximately 6% of all documents processed across our network as fraudulent last year. That is roughly one in sixteen documents showing signs of manipulation, fabrication, or misrepresentation.

This report synthesizes what we learned in 2025 from three sources: detection data from the Inscribe network spanning millions of documents across banks, credit unions, fintechs, and lenders; a survey of 90 fraud and risk leaders conducted in November and December 2025; and interviews with practitioners including senior underwriters, chief risk officers, fraud managers, and industry experts.

The findings point in a clear direction. Document fraud is accelerating. Manual review is reaching its limits. And organizations that adapt will pull ahead of those that do not.

But this is an evolution, not defeat. The same AI capabilities fraudsters use to create convincing fakes can be deployed to detect them. The fraud fighters we interviewed are not discouraged.

(Click the heading link to read more.)



Voice Clones and Bank Fraud: New Risks for CFIs

Source: PCBB BID Daily Newsletter

Voice fraud is on the rise, and so is the quest for defenses by financial institutions. Thanks to artificial intelligence (AI), voice clones are increasingly realistic and being used by scammers against individuals and businesses.

In a recent report from Banking Dive and Modulate, 84% of financial services and retail organizations surveyed said their organizations had experienced moderately to highly sophisticated voice attacks in the past year. About 87% were from fraudsters impersonating customers, and 84% were impersonating employees.

Why AI Voice Fraud Is a Growing Risk

More than half of voice fraud victims reported an average loss per successful incident ranging from $5K to $25K. However, the unseen cost is how much time and energy companies spend trying to combat this expanding and persistent threat. A shocking 8 of 10 respondents said they spent at least 51 hours each year investigating voice fraud cases.

What Most Financial Institutions Are Doing Today

Financial institutions (FIs) are, of course, fighting back. Nearly every FI uses at least one voice fraud detection/prevention method, and most are using three or more as the attacks have grown more sophisticated with the rise of AI.

(Click the heading link to read more.)