FRAUD PREVENTION FRIDAY

Community Bankers of Michigan

Friday, February 20, 2026

Warning: A LinkedIn Phishing Campaign is Targeting Executives

Source: Knowbe4

A phishing campaign is abusing LinkedIn private messages to target executives and IT workers, according to researchers at ReliaQuest. The messages attempt to trick victims into opening an archive file, which will install a legitimate pentesting tool.

"A critical element of this attack was the use of a legitimate, open-source Python script designed for pentesting," ReliaQuest says. "Relying on publicly available tools means less effort for attackers and allows them to reduce costs and detection risks—all while lowering the technical barrier to entry."

The researchers stress that the abuse of legitimate tools makes the campaign more likely to bypass security defenses.

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

Top News

Smart Ways Community Banks Can Address Card Fraud

Source: ICBA Independent Banker

Card fraud is rising and community banks are feeling the impact. Learn how the right mix of technology, staff training, collaboration, and customer education can help banks detect fraud faster, reduce losses, and protect customer trust.

According to data from the Federal Trade Commission, consumers reported losing more than $12.5 billion to fraud in 2024—a 25% increase over the previous year. Consumers aren't the only victims: The 2025 Conference of State Bank Supervisors Annual Survey of Community Banks found that card fraud was the most common and costliest of all fraud experienced by community banks; 59% of reported fraud cases and 39% of reported losses fell into this category.

In 2024, a survey by Federal Reserve Financial Services found that incidents with debit cards caused the largest year-on-year increase in fraud losses for financial institutions. Credit card losses were considerably lower, flagging debit cards as perhaps the biggest vulnerability for banks.

The digital problem

With the rise of e-commerce, card fraud is increasingly digital.

"We're seeing a shift from traditional card-present fraud to more sophisticated account takeover and synthetic identity-based fraud," says Scott Anchin, senior vice president of strategic initiatives and policy at ICBA. "Fraudsters are operating in highly organized ways, making heavy use of digital channels and underground sources of authentication and identity data."

(Click the heading link to read more.)

The Challenge of Balancing Fraud Mitigation and Customer Experience

Source: ProSight

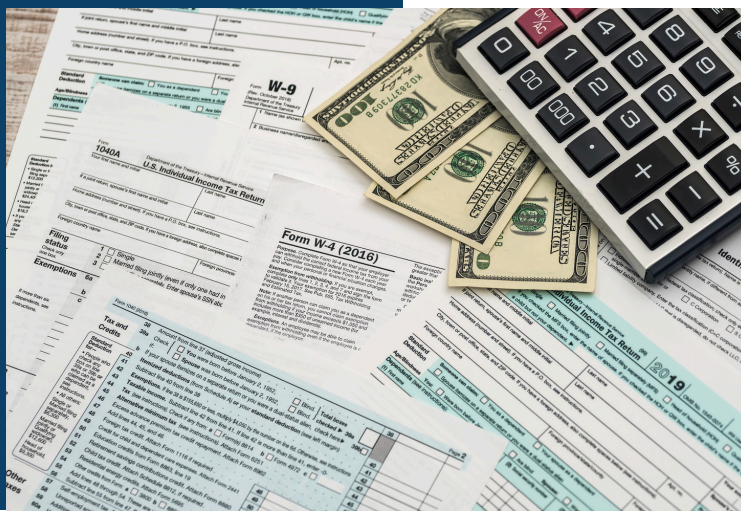
How do banks measure success when it comes to balancing fraud mitigation and customer experience? Every financial institution is different, and there's not one standardized formula. Many start with the fraud loss number — bottom line dollars out the door due to fraud.

The issue here is that not every loss can be clearly attributed to fraud. Some cases ultimately fall into bad debt or loan charge-offs instead. Bartolacci notes that fraud-avoidance metrics may offer a better view of a fraud team's impact, even though they are just as difficult to measure. Fraud-avoidance figures demonstrate preventative value, while fraud-loss numbers reflect actual losses — two distinct but equally important measurements.

Most institutions look at fraud losses versus attrition and abandonment rates, which can be attributed to poor customer experience. The balance, of course, lies in the tradeoff between fraud control and customer convenience. "A lot of institutions are looking at how they balance that out, making sure that their fraud losses are under control in a manageable number, while also ensuring their abandonment rate and attrition rate isn't going above industry expectations," explains Nelson.

To understand the challenge, consider common controls like one-time passcodes. When one-time passcodes were new to consumers around two decades ago, they were often seen as cumbersome — especially to those without a mobile phone.

(Click the heading link to read more.)



Protecting Customers From Income Tax Fraud: A Community Bank's Guide for Tax Season

Source: Community Bankers of Michigan

Tax season is one of the busiest and riskiest times of the year for consumers. As customers gather sensitive documents, file returns, and await refunds, fraudsters exploit this period of high activity and heightened anxiety. Income tax fraud continues to escalate, with criminals leveraging identity theft, phishing, and even AI-enhanced impersonation to steal refunds or gain access to financial accounts. Recent reports indicate that income tax identity theft remains one of the most common and damaging schemes, often involving stolen Social Security numbers used to file fraudulent returns before the legitimate taxpayer has a chance to file theirs. At the same time, scammers increasingly rely on sophisticated impersonation techniques, including fake IRS communications and voice-cloned phone calls, to trick customers into disclosing sensitive information or making urgent payments.

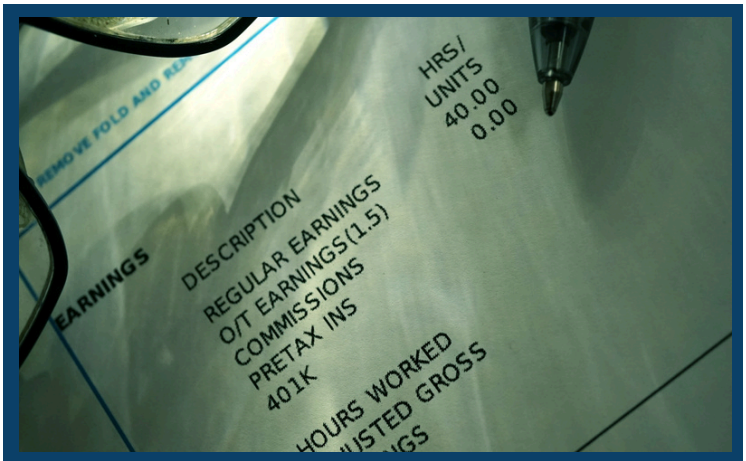
Community banks are uniquely positioned to safeguard customers during this vulnerable period. By educating customers, monitoring suspicious activity, and fostering open communication, banks can prevent fraud before it occurs and reinforce their role as trusted financial partners.

Common Tax Fraud Schemes Targeting Bank Customers

IRS Impersonation Scams

Fraudsters frequently pose as IRS agents through phone calls, emails, or text messages. These messages often demand immediate payment, threaten legal action, or claim there is an issue with a tax return. However, the IRS does not initiate contact through phone, email, or text for sensitive matters, making these requests clear red flags.

(Click the heading link to read more.)



Warning - AI Paystubs Are Here And Its Getting Bad

Source: FrankonFraud

Deepfakes are bad. Very bad. But something else is brewing, and its not looking good.

A new study from Inscribe, a document fraud detection company, found that AI-generated fraudulent documents increased nearly 500% between April and December of 2025.

The finding confirms what fraud investigators have feared – the technology that powers chatbots, voice clones and deepfakes has become a weapon of choice for fraudulent paystubs and bank statements.

But the report reveals that the use of AI is not really what people think.

"AI-Assisted Fraud" Is The Real Problem

Creating convincing paystubs used to require skill. Fraudsters needed Photoshop expertise, access to real document templates and enough knowledge of how to make the math add up for deductions.

With Gen-AI, fraudsters now use AI for the heavy lifting, completely replacing the need for any photoshop expertise whatsoever.

"The real issue right now is AI-assisted document fraud," said Ronan Burke, CEO and Co-Founder of Inscribe. "It's not AI magically generating perfect paystubs. It's people using AI to smooth out the fonts, alignment, wording, and internal consistency so a forged document looks legitimate at a glance."

(Click the heading link to read more.)