FRAUD PREVENTION FRIDAY

Community Bankers of Michigan

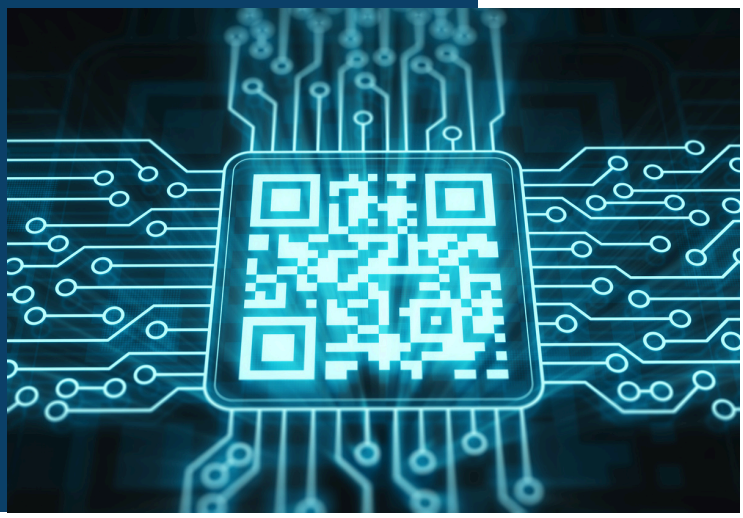
Friday, January 24, 2025

Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud

The FBI is warning the public that criminals exploit generative artificial intelligence (AI) to commit fraud on a larger scale which increases the believability of their schemes. Generative AI reduces the time and effort criminals must expend to deceive their targets. Generative AI takes what it has learned from examples input by a user and synthesizes something entirely new based on that information. These tools assist with content creation and can correct for human errors that might otherwise serve as warning signs of fraud. The creation or distribution of synthetic content is not inherently illegal; however, synthetic content can be used to facilitate crimes, such as fraud and extortion.1 Since it can be difficult to identify when content is AI-generated, the FBI is providing the following examples of how criminals may use generative AI in their fraud schemes to increase public recognition and scrutiny.

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

Top News



Scam Alert: QR Code or an Unexpected Package

An unexpected package from an unknown sender arrives in your name. You open it and find a note that says it's a gift, but it doesn't say who sent it. The note also says to scan a QR code to find out who sent it — or to get instructions on how to return it. Did someone really send you a gift? Or is it an attempt to steal your personal information?

If you know it's really a gift, you can keep it. But know that the unexpected package could be a new twist on a brushing scam that could steal your personal information.

If you scan the QR code, it could take you to a phishing website that steals your personal information, like credit card numbers or usernames and passwords. It could also download malware onto your phone and give hackers access to your device.

If you scanned the QR code and entered your credentials, like your username and password, into a website, change your password right away. Create a strong password that is hard to guess, and turn on two-factor authentication.

If you're concerned someone has your personal information, get your free credit report at AnnualCreditReport.com. Look for signs that someone is using your information, like accounts in your name you don't recognize. (You can get a free credit report every week.)

Also review your credit card bills and bank account statements and look for transactions you didn't make. And consider taking other steps to protect your identity, like freezing your credit or putting a fraud alert on your credit report.

If you think someone stole your identity, report it, and get a personal recovery plan at IdentityTheft.gov.

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

CBM Associate Member Visa Shares Biannual Threats Report

This report provides an overview of the top payments ecosystem threats within the past six-month period (January – June 2024) as identified by Visa Payment Fraud Disruption (PFD). In the December 2023 Biannual Report, Visa PFD noted an interesting shift in threat actors' organization, access to tools, and target choice, with threat actors increasing in their scope of abilities and sophistication given advances in technology. The past six-month period saw a continuation of these expanding trends in cross-sector collaboration and ingenuity, with a specific targeting two aspects of the ecosystem: 1) system misconfigurations and vulnerabilities and 2) cardholders.

Threat actors continue to probe the payments ecosystem for vulnerabilities and were successful in conducting fraud schemes affecting multiple financial institutions, technologies, and processes. An example of this impact is the erroneous approval of fraudulent transactions. These transactions are approved due to a mishandling of the authorization process and are used to initiate Purchase Return Authorization (PRA) attacks. Visa PFD opened a record number of PRA investigations over the past six months, an 81% increase from the previous six-month period. Per successful attack, each of these fraud operations have resulted in potential losses of nearly US$184K for Visa's issuing partners.

Enumeration attacks remain a popular vector for threat actors to validate and compromise payment credentials, resulting in significant follow-on fraud. Over the past six months, the US region increased as the most heavily targeted region from the issuing side (58% of total issuer enumeration, increase of 16% from the same period in 2023), but decreased from the acquiring side (61% of total acquiring enumeration, decrease of 3% from the same period in 2023).

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

Overseeing Third-Party Vendors' Cybersecurity

While the use of outside vendors can create powerful partnerships and allow for vast capabilities, it's important to remember that your third-party vendors' security is your security. For that security to be effective, you must still conduct thorough due diligence and remain vigilant in your oversight of the third party's practices.

The following are ways your institution can best reduce third-party cyber risk:

- Routinely review vendor service policies and controls. Currently, only half of the financial institution executives surveyed investigate their third-party cybersecurity policies and procedures — and only 51% even require that cybersecurity policies exist. Institutions should not only conduct thorough due diligence before they contract with third-party cybersecurity providers, but they should then also regularly monitor and review the provider's policies, systems, and security controls. Two good places to start are with **SOC 2** reports and ISO certifications.
- Ensure security breach protocols are addressed. For vendors that are engaged in high-risk activities, financial institutions should ensure that their responsibilities and activities are clearly defined and included in their service contracts. Vendors should be required to have information security programs and clear guidelines on security breach protocols, particularly around swiftly notifying financial institutions of data breaches and protections against financial losses from a breach. Right now, only half of banking executives surveyed have their financial institutions mandate a prompt alert when a breach occurs, and 43% investigate a breach's incident history. Some vendors consider full documentation of their Information Security Program, including breach response, proprietary. If this is the case, request summary documents or a table of contents for breach response reports and ensure you have the latest update.

(Click the heading link to read more.)

From Onboarding to Compliance: HR's Power in Cybersecurity Protection

Cybersecurity is a growing concern for organizations across all industries. On average, businesses paid $1.5 million to recover from a ransomware attack and it took, on average, one month to fully recover. It's not just large companies being targeted; small businesses are often targeted by cybercriminals due to their limited resources and less robust security measures. While IT departments are typically tasked with implementing cybersecurity measures, Human Resources (HR) departments play a critical role in fostering a security-conscious culture within the organization.

Less than 1% of companies with under 500 employees have someone dedicated to cybersecurity, making them extremely vulnerable. "Cybersecurity isn't just for large organizations—it's critical for every business," said Rick Snyder, CEO of SensCy, ASE's newest partner. HR must work across the organization to protect employee info as well as other valuable, secure company data.

(Click the heading link to read more.)