Community Bankers of Michigan Regulatory Dispatch
September 9, 2026

Timely news and resources community bankers can use

Scam Likely: It's a Good Thing We Have Fraud Insurance… Right?! – Miller Nash LLP

Welcome back to the latest installment of our "Scam Likely" series, where we examine recent scams, frauds, and other financial crimes. It has been some time since our last installment, but just when you thought you were out, the risk of fraud loss pulls you back in.

This installment of our series was prompted by a recent Summer Threat Spotlight Alert issued by the FDIC. In that Alert, the FDIC warns banks to take a close look at their fraud insurance policies. The insurance industry has been busy updating their policies to narrow the instances of what is, and what is not, covered in the case of a fraud loss. If a bank unwittingly fails to satisfy its policy's requirements, it risks losing coverage.

The Set Up

It is early Wednesday morning. Your bank customer cannot remember their online banking password, so they submit a reset request. Your online banking system applies its multi-factor authentication procedure, and the customer successfully changes their password. A few days later, the customer initiates a $100,000 wire transfer through online banking – the size of this wire transfer is typical for the customer. As always, your trusty team applies its normal wire transfer security procedures (*e.g.*, a callback, MFA, dual control, etc.) and processes the payment.

On Monday morning, you get a phone call from a very upset customer that last week's wire transfer was unauthorized and fraudulent. As you likely guessed, the customer fell victim to a business email compromise or account takeover, and the wired funds are long gone. Your customer is now looking to the bank to cover the loss and recredit their account. You think to yourself: "Even if this is on us, we have insurance for this… right?"

Comment: A recent FDIC alert highlights that insurers have tightened policy requirements, and banks may lose coverage if they fail to follow every condition in their insurance policies. Fraud insurance provides a financial safety net, but insurers frequently deny claims when policyholders fail to meet precise and rigid security protocols. Consequently, securing a payout requires flawless execution and documentation of every verification requirement before any scam occurs.

CBM Insights

Q: Returned Mail- currently we log in the returned mail and try to contact the customer. We keep the returned mail in a box, and it keeps accumulating. My question is: do we have to keep the statements stored, or can we make a note on the system as an alert and shred the statements? We can always reprint them if customers request them.

Hold Statements- is there a liability when we hold statements? We currently have statements that are on hold, and customers are not picking them up.

A: Regarding returned mail, there are no rules or regulations on how you process, rather it is a bank policy and procedural issue. As long as you can recreate the mailing's contents, there is no reason to hold and store returned mail. The better option is to simply shred the returned mail and recreate it if the customer is later located with an updated address or requests a copy. Returned envelopes contain sensitive customer data, such as account numbers, balances, and Social Security numbers. Leaving physical documents in storage or mail trays makes them vulnerable to theft or internal data leaks, so destruction and recreation is a better option.

Regarding hold statements, again, there are no rules or regulations on how you process; it is both a bank policy and procedural issue and a contract issue. In other words, what does your deposit agreement or agreement to hold mail provide for?

Regarding statements in general, only Regulation E specifically addresses a requirement to provide a statement. See below:

(b) Periodic statements. For an account to or from which electronic fund transfers can be made, a financial institution shall send a periodic statement for each monthly cycle in which an electronic fund transfer has occurred; and shall send a periodic statement at least quarterly if no transfer has occurred. The statement shall set forth the following information, as applicable:

Source link.

Most bank deposit contracts include language that the statement will be provided to the last known address (or email address in the event of eStatements) unless updated by the accountholder. ESIGN requires you to disclose the procedures your customer must follow to report email address changes. Under most hold-mail agreements, a customer is legally deemed to have received notice of any fee changes, statements, or account limits the moment the bank places the document in the hold file – so consult legal counsel on that issue.

Finally, regulators view hold mail as a high-risk factor for money laundering and financial crime. It prevents the bank from reliably confirming a customer's active residential or business location.

Bank Management

	FRB Beige Book (09/02/2026) – National Summary - Overall Economic Activity Economic activity increased modestly since early July. Ten of the twelve Federal Reserve Districts reported growth in the slight to moderate range; two Districts reported no change. Consumer spending grew slightly on balance; reports reflected both heightened price sensitivity on the one hand and solid high-end purchases on the other. Auto sales were mostly subdued, dampened by downbeat consumer confidence, high fuel prices, and rising financing costs. Tourism activity increased. Notably, airlines reported strong demand despite higher airfares. Manufacturing activity picked up across most Districts, with some highlighting ongoing strength in demand for defense and data center-related orders. Services firms reported slight to modest increases in activity. Financial conditions improved slightly as loan volumes remained solid or increased across most Districts. Residential construction declined while nonresidential construction increased on balance, with some Districts noting a high concentration of activity related to data center projects. Agriculture conditions saw slight improvement but generally remained strained; the livestock sector was strong while conditions were stressed among crop producers. The general outlook for the coming months was positive, but sentiment was mixed across sectors, with contacts reporting heightened uncertainty surrounding the effects of higher energy prices, policy, and international conflict. Labor Markets Employment rose very slightly overall, with three Districts showing modest gains in employment, four reporting slight gains, and five Districts experiencing no change. Eight Districts saw a change in their pace of growth from the previous report, but there was less overall dispersion among Districts. Healthy labor demand was seen most frequently in manufacturing, construction, and some service sectors, while retail and hospitality sectors

	saw falling labor demand. Labor availability was mixed. Skilled trades and technical workers were difficult to find. Districts also reported both positive and negative effects of artificial intelligence on labor demand. Wage growth was modest to moderate in most Districts. Significant wage increases were most often connected to demand for skilled workers in construction and manufacturing. Prices Prices increased moderately in eight Districts, with two Districts reporting modest increases, one slight increase, and one robust increase. Compared with the previous reporting period, the pace of price increases was the same in eight Districts, decreased in three, and increased in one. Input price pressures were notably elevated in manufacturing and construction across multiple Districts, with widespread reports of price increases for energy, transportation, and raw materials, particularly metals and petrochemicals. Retail and manufacturing contacts continued to note tariff-related impacts in multiple Districts. Firms also broadly reported significant health care and insurance cost pressures. Consumer-facing contacts in a few Districts noted that heightened price sensitivity among customers was putting a limit on their ability to pass through input price increases.
	OCC Registration Open for Community Bank Director and Senior Management Fall 2026 Workshops (09/01/2026) – WASHINGTON—The Office of the Comptroller of the Currency (OCC) is accepting registrations for its upcoming 2026 in-person workshops for board directors and senior management of OCC-supervised community banks. The fall workshops are the final in-person workshop offerings planned for 2026, and include the new Asset Management workshop, which provides a comprehensive overview of asset management activities, key responsibilities and expectations, exam process, and effective oversight and risk management practices. The OCC examiner-led workshops provide practical training and guidance related to the challenges that directors and senior management face every day, reinforcing the agency's commitment to supporting and strengthening community banks. The date, title, and location of in-person workshops for upcoming 2026 are:

Dates	Workshop Name	Location
September 15	Risk Governance	Longview, Texas
September 16	Capital Markets	Longview, Texas
September 29	Compliance Risk	Cleveland, Ohio
September 30	Credit Risk	Cleveland, Ohio
October 6	Operational Risk	Tulsa, Oklahoma
October 7	Compliance Risk	Tulsa, Oklahoma
October 14	Asset Management	Denver, Colorado
October 20	Asset Management	New York, New York
November 4	Building Blocks	Indianapolis, Indiana

Comment: These are excellent training opportunities for national bank directors and senior management.

BSA / AML

FinCEN Identifies Nearly $13 Billion Linked to Suspected Digital Asset Scams Operated by Overseas Scam Centers (09/03/2026) – **WASHINGTON**—The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) published an analysis and an alert to financial institutions to be vigilant to digital asset investment scams perpetrated by overseas scam centers. The action is the latest in Treasury's efforts to protect Americans from fraud.

Digital asset investment scams—also known as "pig butchering," "romance baiting," or "cryptocurrency confidence schemes"—are sophisticated fraud operations. Criminals use fake personas and social engineering tactics to manipulate victims, who are often American, into transferring funds to fraudulent digital asset investments. These scams are largely perpetrated by transnational criminal organizations based in Southeast Asia, which operate industrial-scale scam compounds and leverage vast networks of criminal actors to facilitate and profit from scams.

"Digital asset investment scams pose one of the most significant fraud threats facing Americans," said **Gene Lange, who is performing the duties of Under Secretary for Terrorism and Financial Intelligence**. "The transnational criminal organizations behind these scams exploit both emerging technologies and human vulnerabilities, resulting in devastating financial losses for innocent American victims."

Bank Secrecy Act (BSA) Reports Highlight Rising Rate of Suspected Scam Activity

- As discussed in the FTA, FinEN analyzed 33,904 BSA reports involving suspected digital asset investment scam-related activity filed between September 8, 2023, and December 31, 2025, totaling approximately $12.7 billion in financial activity tied to suspected digital asset investment scams.
- Individuals of all ages were the target of suspected digital asset investment scams across all 50 states and several U.S. territories, according to BSA reports.
- Analysis of BSA reporting indicated use of a variety of well-known fraud tactics. Illicit actors often used assumed names or identities to pose as potential romantic partners, new friends, or new business partners to target scam victims. Scammers often created websites and mobile applications that imitated legitimate investment services to carry out their criminal activity.

Scam Center Operators Use "Guarantee Marketplaces" and Professional Money Launderers to Facilitate Illicit Activity

- Guarantee marketplaces are online markets where scam center operators purchase illicit services, such as online account creation, phishing, and money laundering services.
- Scam center operators use professional money launderers to establish financial accounts and shell companies, as well as to move funds.
- Professional money launderers integrate scam proceeds into the formal financial system through networks of money mules and through stablecoin transfers to digital asset exchanges outside of the United States.

Alert Identifies Key Indicators of Illicit Activity Linked to Scam Centers

- FinCEN has identified red flags to help financial institutions detect, prevent, and report suspicious activity connected to scam centers. BSA reporting is essential to supporting law enforcement investigations and victim recovery efforts.
- FinCEN strongly encourages financial institutions to participate in voluntary information sharing under Section 314(b) of the USA PATRIOT Act, which allows institutions to share information regarding activities that may involve money laundering or terrorist activity while receiving safe harbor protections from liability.

As the financial intelligence unit (FIU) of the United States, FinCEN operates a Rapid Response Program, using its authority to share financial intelligence rapidly with counterpart FIUs and encourages foreign authorities to stop and repatriate the fraudulent transactions using authorities under their respective legal and regulatory frameworks. Victims of cyber-enabled fraud should immediately contact their financial institution and file a complaint with the FBI's Internet Crime Complaint Center (IC3) and/or the nearest U.S. Secret Service field office.

	This Alert and Financial Trend Analysis aim to defend the U.S. financial system against cybercrime, fraud, and predatory schemes, an objective of Executive Order 14390, "Combatting Cybercrime, Fraud, and Predatory Schemes Against American Citizens." **Resources:** • FinCEN Alert on Money Laundering Activity Associated with Digital Asset Investment Scam Centers • Financial Trend Analysis: Digital Asset Investment Scams: 2023-2025 Threat Pattern & Trend Information ***Comment: FinCEN identified $12.7 billion in suspicious transactions tied to Southeast Asian digital asset investment scams operated by transnational criminal networks. These industrial-scale operations utilize forced labor to target victims nationwide through fraudulent trading platforms and messaging apps.***
	FinCEN Updates: FinCEN Reissues Order Requiring Transparency from MSBs Along Southwest Border (09/02/2026) – **WASHINGTON**—The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) reissued a Geographic Targeting Order (GTO) to help law enforcement combat illicit activity and associated money laundering by Mexico-based cartels and other criminal actors along the southwest border of the United States. The GTO subjects certain money services businesses (MSBs)—which provide financial services outside of a formal bank—to enhanced reporting requirements with FinCEN. "Mexico-based drug cartels have flooded our borders with narcotics and poisoned thousands of Americans," said **Secretary of the Treasury Scott Bessent**. "Under President Trump's leadership, Treasury is continuing to dismantle the cartels. The reissued Geographic Targeting Order will ensure law enforcement has the actionable data they need to follow the money." The reissued GTO underscores the Trump Administration's deep concern with the significant risk to the U.S. financial system presented by cartels, drug traffickers, and other criminal actors along the southwest border. The GTO requires MSBs to file Currency Transaction Reports with FinCEN for cash transactions between $1,000 and $10,000 occurring in specific ZIP codes in Bernalillo, Dona Ana, and San Juan counties in New Mexico, and Cameron, El Paso, Hidalgo, Maverick, and Webb counties in Texas. The terms of this GTO are effective for 180 days after publication on the *Federal Register*. The reissued GTO will allow investigators to develop leads focused on combatting the flow of drugs into the United States and associated money laundering activity, and it will allow for increased scrutiny of cash transactions along the southwest border. Further, the reissued GTO will ensure local, state, and federal law enforcement can deny individuals and entities associated with drug trafficking organizations access to the U.S. financial system. Questions about the GTO should be directed to www.fincen.gov/contact.

	Resources • Reissuance Southwest Border Geographic Targeting Order ***Comment: This reissued Geographic Targeting Order (GTO) requires money services businesses in specific southwest border counties to report cash transactions starting at a lowered threshold of $1,000. Effective through March 1, 2027, this regulatory action aims to disrupt illicit cartel networks by tracking lower-dollar financial trails often used in cross-border smuggling and money laundering. For awareness and information sharing.***
	Joint Statement on Suspicious Activity Report Confidentiality Considerations Regarding Communications with Customers (09/02/2026) – The Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the Office of the Comptroller of the Currency (collectively, the Agencies), and the Financial Crimes Enforcement Network are issuing this statement to clarify confidentiality requirements related to Suspicious Activity Reports (SARs). This joint statement is particularly relevant when banks communicate with their customers regarding potentially fraudulent transactions, other suspicious activity (e.g., payment fraud, including check fraud), or account closures. **Statement of Applicability:** The contents of, and material referenced in, this FIL apply to all FDIC-insured financial institutions. Highlights: • The Bank Secrecy Act (BSA) prohibits the disclosure of a SAR or information that would reveal the existence of a SAR, including to a customer or other person who is the subject of the SAR. However, the joint statement clarifies that the BSA and its implementing regulations do not prohibit banks from communicating with a customer or other person who is the subject of a SAR or with other third parties, including other banks, about potentially fraudulent or other suspicious transactions involving the customer's account or notifying the customer of the bank's intention to close the account for potentially fraudulent or other suspicious activity, so long as that communication does not reveal the existence of a SAR. • In general, banks should consider customer communication on a case-by-case basis and take precautions when discussing information that could reveal the existence of a SAR. FIL-55-2026 Attachment(s) Joint Statement on SAR Confidentiality (PDF) ***Comment: The Joint Statement clarifies that banks can discuss fraud or account restrictions directly with customers without violating Bank Secrecy Act rules. However, internal teams must ensure these conversations never reveal that a Suspicious Activity Report has been filed or is under consideration. You can review the details on the issuing agency's official platform.***

Deposit / Retail Operations

FTC See a QR code parked somewhere? Don't scan it…yet! (09/03/2026) – Ever tried to pay for parking and discovered you need to scan a QR code to pay? It seems like a convenient way to pay, but it turns out scammers like using QR codes, too. People have reported scammers covering up legit QR codes on parking meters with a QR code of their own. If you scan that scammy QR code, it could take you to a fake site designed to steal your money, your personal information, or both. So, how can you protect yourself from these scams?

Comment: The Federal Trade Commission warns that scammers are placing fraudulent QR code stickers over legitimate ones on parking meters to harvest financial and personal information. Users are advised to inspect parking meters for tampering and utilize official municipal applications for payment rather than scanning arbitrary codes.

Human Resources

No news to report this week.

Lending

OCC Releases CRA Performance Evaluations for 23 National Banks and Federal Savings Associations (09/01/2026) – WASHINGTON—The Office of the Comptroller of the Currency (OCC) released a list of Community Reinvestment Act (CRA) performance evaluations that became public during the period of August 1, 2026, through August 31, 2026.

Under the CRA, the OCC assesses an institution's record of meeting the credit needs of its entire community, including low- and moderate-income neighborhoods, consistent with the safe and sound operation of such institution.

Technology / Security

CISA, FBI International Partners Release Guidance on Effective Communication During Service Outages (09/02/2026) – The Cybersecurity and Infrastructure Security Agency (CISA), in collaboration with the Federal Bureau of Investigation (FBI) and international partners, released joint guidance Communicating Under Pressure: Best Practices for Service Providers to help organizations plan to communicate clearly and effectively during service outages impacting IT and operational technology (OT) systems.

Whether caused by cyber threat actors, human error, equipment failure, or natural hazards, service outages can create disruption and societal panic even without speculation from end users and the public as added factors. Outages at one organization may cascade across interconnected systems, increasing the uncertainty and potential for panic. This guidance describes how service providers can prepare and execute clear, timely, and audience-appropriate messaging that articulates accurate information while still aligning with operational security, law enforcement, and containment efforts.

Key actions for communicating during service outages:

- Lead with confirmed facts, scope, and affected systems
- Tailor updates to each audience
- State what is known, unknown, and under investigation
- Explain operational impact and any customer actions
- Avoid vague language, speculation, and public relations "spin"
- Provide frequent, time-stamped updates
- Align messaging with legal, regulatory, and law enforcement requirements

CISA's CI Fortify initiative provides information and resources that help critical infrastructure organizations prepare to isolate and recover their vital OT systems during a major cyber incident or crisis. Changes in service availability, whether from outages or isolation as a defensive strategy, require transparent and ongoing communication to help end users minimize operational impact, limit speculation, and preserve trust. For emergency planning purposes, critical infrastructure owners and operators should assume that telecommunications services may be disrupted or otherwise unreliable, making it crucial for organizations to have crisis communications plans in place that integrate backup communication methods and understand the type of communication they should expect from their service providers.

Read the guidance to learn more about crisis communications planning.

Comment: CISA, the FBI, and international partners released this joint guide outlining best practices for critical infrastructure and technology providers to communicate effectively during major outages. The guidance emphasizes clarity, transparency, and early preparedness to maintain public trust and deliver actionable technical updates during system failures. For more information, visit CISA.

Wired ATM Flaws Reveal Key Weaknesses in the Software Supply Chain (08/31/2026) – For the past five years, security researcher Matt Burch has immersed himself in the esoteric and high-stakes world of ATM security, in which small software flaws can sometimes expose cold, hard cash. As Burch has bored deeper into the computers powering these digital lock boxes—and continued to find vulnerabilities in key digital security systems—he has started working to raise the alarm, not just about overlooked ATM flaws, but about how that same software used in other industries can introduce weaknesses in an array of critical systems.

At the Black Hat and Defcon security conferences in Las Vegas this month, Burch presented findings about nine vulnerabilities that have been fixed in disk encryption and pre-boot authentication software called CryptoPro Secure Disk. The flaws could have been exploited to bypass CryptoPro's integrity checks and gain full access to encrypted devices.

	Comment: Security researcher Matt Burch discovered nine vulnerabilities in CryptoPro Secure Disk, a disk encryption and pre-boot authentication software produced by German firm CryptWare. While the software is used in ATMs—such as Diebold Nixdorf's Vynamic Security Suite—it is also widely deployed across embedded devices, enterprise Microsoft Windows environments, healthcare, automotive, and government sectors.

Open for Comment

Included only when specific to or relevant for community banks to comment on. Date posted may not be the same as the Federal Register Date.

08.27.2026 **FDIC** Reciprocal Deposits: Implementing the 21st Century ROAD to Housing Act SUMMARY: The Federal Deposit Insurance Corporation (FDIC) is amending its brokered deposit regulations to conform with recent changes to section 29 of the Federal Deposit Insurance Act made by section 902 of the 21st Century ROAD to Housing Act related to reciprocal deposits, which took effect on July 11, 2026. The FDIC is also providing certain clarifications regarding the reciprocal deposit framework to facilitate and simplify compliance. The FDIC invites public comment on this interim final rule. **DATES: The interim final rule is effective September 1, 2026. Comments must be received on or before October 1, 2026.**

07.31.2026 **FDIC** Extensions of Credit to Insiders SUMMARY: The Federal Deposit Insurance Corporation (FDIC) is proposing to increase quantitative thresholds for certain extensions of credit to insiders of FDIC supervised institutions, as restricted by the Federal Reserve Act and regulations promulgated thereunder. Specifically, the proposal would increase the thresholds for certain (1) extensions of credit to executive officers not otherwise specifically authorized by statute from $100,000 to $400,000; and (2) extensions of credit to insiders requiring prior approval by the board of directors from $500,000 to $2,000,000. The proposal would also establish an indexing methodology to periodically update such thresholds over time. **DATES: Comments must be received on or before October 5, 2026.**

07.31.2026 **Joint** Community Reinvestment Act Regulations SUMMARY: The Office of the Comptroller of the Currency (OCC) and the Federal Deposit Insurance Corporation (FDIC) are proposing to amend their Community Reinvestment Act rules by making certain substantive, technical, and process-oriented changes to refocus on the statutory objective of encouraging banks to meet the credit needs of their communities; to better ensure that community development grants reach the communities they are intended to benefit; to reduce unnecessary burden, particularly for community banks; and to provide greater clarity for how to obtain CRA consideration. The OCC and the FDIC are also proposing certain technical changes to their rules implementing the Community Reinvestment Act sunshine requirements of the Federal Deposit Insurance Act. In addition, the OCC is proposing similar technical changes to its Public Welfare Investments rule and its Rules, Policies, and Procedures for Corporate Activities. **DATE: Comments must be received on or before October 13, 2026.**

07.17.2026 **FDIC** Reporting Forms and Instructions Associated with Requirements and Standards for FDIC Supervised Permitted Payment Stablecoin Issuers SUMMARY: The FDIC invites comment on new forms and instructions associated with an Office of Management and Budget (OMB) control number (3064-0225) assigned in connection with a notice of proposed rulemaking. In accordance with the requirements of the Paperwork Reduction Act of 1995 (PRA), the FDIC may not conduct or sponsor, and the respondent is not required to respond to, an information collection unless it displays a currently valid OMB control number. As part of the notice of proposed rulemaking, the FDIC sought a new OMB control number for a new information collection that would include weekly and quarterly reporting forms that must be completed by permitted payment stablecoin issuers. **DATES: Comments must be submitted on or before September 18, 2026.**