50TH
ANNIVERSARY
1974 CBM 2024
Community Bankers of Michigan

Community Bankers of Michigan Regulatory Dispatch

June 20, 2024

Timely news and resources community bankers can use

to better stay on top of a rapidly changing world.

FRB Stomp out Scams with the ScamClassifier Model

To help combat the growing prevalence and severity of scams, the Federal Reserve and a work group of payments and fraud experts developed a new tool to improve scam reporting, detection and mitigation.

The newly released ScamClassifier model supports consistent and detailed classification, reporting, analysis and identification of scams, attempted scams and related trends.

Similar to the FraudClassifierSM model announced by the Federal Reserve in 2020, the ScamClassifier model uses a series of questions to differentiate and classify scams and attempted scams by category and type. Voluntary adoption of the ScamClassifier model can improve scam detection, investigation and mitigation, as well as expedite scam claims intake and improve scam reporting.

Stay informed of the Fed's efforts to support payments security and mitigate fraud by exploring FedPaymentsImprovement.org.

Comment: The ScamClassifier Model, like the FraudClassifier Model released in 2020, is a voluntary tool that banks can integrate into their existing classification and case management systems. The Federal Reserve encourages banks and other stakeholders to evaluate their current processes and consider how the models can enhance their anti-scam and anti-fraud efforts.

Items of Interest

Bank Management

🟨	**CFPB** Laying the Foundation for Open Banking in the United States (06/12/2024) – New digital banking technologies have the power to expand and open market access for American consumers and emerging

🟨	businesses. In a more competitive market, Americans will be able to earn higher rates on their savings, pay lower rates on their loans, and more efficiently manage their finances. But the new technologies, and the competition they can fuel, have not yet reached their full potential. Consumers continue to encounter all too familiar obstacles when trying to switch banks or apply for loans. The CFPB is working to accelerate the shift to open banking through a new personal data rights rule intended to break down these obstacles, jumpstart competition, and protect financial privacy. To do this, the CFPB is formalizing an unused legal authority enacted by Congress in 2010. This authority gives consumers the right to control their personal financial data. These rights will become a practical reality after the CFPB implements a rule that sets expectations for the market. We expect to solicit comments on our formal proposal in a few months and to finalize it in 2024. But the agency must not micromanage open banking. Fair standards developed by the market to leverage our rule will be critical to the creation and maintenance of an open banking system in which consumers can vote with their feet -- and exercise their data rights without being trapped by powerful incumbents and without losing control of their data. Our proposal will recognize that the CFPB must resolve certain core issues because system participants are deadlocked or because existing approaches do not put consumers fully in the driver's seat. But many of the details in open banking will be handled through standard-setting outside of the agency. Properly pursued, such standards can allow open banking to evolve as new technologies emerge, new products develop, and new data security challenges arise. To thrive, standard-setting organizations must not skew to the interests of the largest players in the market. They must reflect the full range of relevant interests — consumers and firms, incumbents and challengers, and large and small actors. In consumer finance, powerful firms have sometimes looked to manage emerging technologies through utilities, networks, or standard setting organizations skewed to their interests – or even owned by them. Control of the open banking system by such players threatens competition and the consumer's control of their own financial affairs. While the CFPB intends for the market to play a significant role in developing and maintaining open banking standards, it will pay close attention to any attempts to limit consumers' exercise of their data rights, particularly where such attempts proceed from coordinated efforts by dominant firms. As the CFPB expects fair standards to play a critical role in open banking, our proposed rule will seek to take appropriate account of that role. We continue to encourage those seeking to develop industry open banking standards in the United States to discuss their plans with the CFPB so that those standards appropriately allow consumers to exercise their personal financial data rights. ***Comment: For the smallest banks - those with less than $850 million in total assets - the compliance deadline will be four years from the effective date of the Final Rule.***

BSA / AML

🟩	**FinCEN** Reminds Financial Institutions to Remain Vigilant to Elder Financial Exploitation (06/14/2024) – WASHINGTON—As the nation recognizes World Elder Abuse Awareness Day, the Financial Crimes Enforcement Network (FinCEN) reminds financial institutions to remain vigilant in identifying and reporting suspicious activity related to elder financial exploitation (EFE). EFE-related losses affect personal savings, checking accounts, retirement savings, and investments, and can severely impact victims' well-being and financial security as they age. FinCEN has previously published resources to help stakeholders combat EFE.

🟩	Earlier this year, FinCEN issued an analysis focusing on patterns and trends identified in Bank Secrecy Act (BSA) data linked to EFE, which indicated roughly $27 billion in EFE-related suspicious activity. FinCEN examined BSA reports filed by financial institutions between June 15, 2022 and June 15, 2023 where filers either used the key term referenced in FinCEN's June 2022 EFE Advisory or checked "Elder Financial Exploitation" as a suspicious activity type. This amounted to 155,415 filings from financial institutions. In addition to filing a Suspicious Activity Report, FinCEN recommends that financial institutions refer customers who may be victims of EFE to the Department of Justice's National Elder Fraud Hotline at 833-FRAUD-11 or 833-372-8311 for assistance with reporting suspected fraud to the appropriate government agencies. EFE victims can file incident reports to the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) and the Federal Trade Commission. For educational resources on EFE and scams targeting older adults, please see the websites of the Consumer Financial Protection Bureau's Office for Older Americans and the Department of Justice. **FinCEN Resources on Elder Financial Exploitation** • Financial Trend Analysis on Elder Financial Exploitation: Threat Pattern & Trend Information, June 2022 to June 2023 (April 2024) • FinCEN Advisory on Elder Financial Exploitation [FIN-2022-A002] (June 2022) ***Comment: Ensure employees are made aware of the FinCEN recommendations and guidance for reporting. In Michigan, the Financial Exploitation Prevention Act requires banks to develop policies and training to identify and report customer exploitation, including freezing accounts under certain circumstances.***
🟩	**FinCEN** Updates Frequently Asked Questions on Beneficial Ownership Information (06/10/2024) – The Financial Crimes Enforcement Network (FinCEN) has updated its Beneficial Ownership Information Frequently Asked Questions about reporting companies and exemptions, beneficial owners, the reporting requirements, and general questions, including information about how the Corporate Transparency Act applies to Indian Tribes. ***Comment: The update includes 5 new FAQs, and provides additional guidance and information about reporting companies and exemptions, beneficial owners, reporting requirements, and general questions, including information about how the Corporate Transparency Act applies to Indian Tribes and Homeowner Associations.***

Deposit / Retail Operations

🟨	**OCC** Prohibition Against Interstate Deposits: Annual Host State Loan-to-Deposit Ratios (06/13/2024) – Summary The Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation (collectively, the agencies) issued on May 31, 2024, the host state loan-to-deposit (LTD) ratios. The OCC is issuing this bulletin to inform banks about how these ratios are used to determine compliance with section 109 of the Riegle—Neal Interstate Banking and Branching Efficiency Act of 1994 (IBBEA). **Rescission:** This bulletin rescinds OCC Bulletin 2023-14, "Prohibition Against Interstate Deposits: Annual Host State Loan-to-Deposit Ratios," published May 19, 2023.

Note for Community Banks:

- Section 109 of the IBBEA applies to community banks that have covered interstate branches.
- Section 109 does not apply to federal savings associations.

Highlights:

These ratios

- use data as of June 30, 2023. The data excludes banks designated for Community Reinvestment Act (CRA) purposes as wholesale, limited purpose, or special purpose banks.
- are used to compare a bank's statewide LTD ratio with the host state LTD ratio for banks in a particular state.
- update data last released on May 19, 2023.

Background:

Section 109 of the IBBEA prohibits the use of interstate branches primarily for deposit production. The OCC's CRA regulation, specifically 12 CFR 25, subpart E, "Prohibition Against Use of Interstate Branches Primarily for Deposit Production," implements the requirements of IBBEA, section 109. The regulation includes specific tests for determining whether an interstate bank is lending appropriately in host states where it has branches.

Section 109 of the IBBEA and 12 CFR 25, subpart E, provide a process to test compliance with the statutory requirements. The first step in the process is an LTD ratio test that compares a bank's statewide LTD ratio with the host state LTD ratio for banks in a particular state. The second step is conducted if a bank's statewide LTD ratio is less than 50 percent of the published host state LTD for that state or if data are insufficient to complete step one. The second step requires the OCC to determine whether the bank is reasonably helping to meet the credit needs of the communities served by the bank's interstate branches. A bank that fails both steps is subject to sanctions by the OCC.

The LTD ratios are published annually and comply with the requirements of IBBEA section 109.

Comment: Section 109 prohibits a bank from establishing or acquiring a branch or branches outside of its home state primarily for the purpose of deposit production. Section 106 of the Gramm-Leach-Bliley Act of 1999 amended coverage of section 109 of the Interstate Act to include any branch of a bank controlled by an out-of-state bank holding company.

Human Resources

No news to report this week.

Lending

CFPB Proposes to Ban Medical Bills from Credit Reports (06/11/2024) – WASHINGTON, D.C. - The Consumer Financial Protection Bureau (CFPB) proposed a rule that would remove medical bills from most credit reports, increase privacy protections, help to increase credit scores and loan approvals, and prevent debt collectors from using the credit reporting system to coerce people to pay. The proposal would stop credit reporting companies from sharing medical debts with lenders and prohibit lenders from making lending decisions based on medical information. The proposed rule is part of the CFPB's efforts to address the burden of medical debt and coercive credit reporting practices.

"The CFPB is seeking to end the senseless practice of weaponizing the credit reporting system to coerce patients into paying medical bills that they do not owe," said CFPB Director Rohit Chopra. "Medical bills on credit reports too often are inaccurate and have little to no predictive value when it comes to repaying other loans."

In 2003, Congress restricted lenders from obtaining or using medical information, including information about debts, through the Fair and Accurate Credit Transactions Act. However, federal agencies subsequently issued a special regulatory exception to allow creditors to use medical debts in their credit decisions.

The CFPB is proposing to close the regulatory loophole that has kept vast amounts of medical debt information in the credit reporting system. The proposed rule would help ensure that medical information does not unjustly damage credit scores and would help keep debt collectors from coercing payments for inaccurate or false medical bills.

The CFPB's research reveals that a medical bill on a person's credit report is not a good predicter of whether they will repay a loan. In fact, the CFPB's analysis shows that medical debts penalize consumers by making underwriting decisions less accurate and leading to thousands of denied applications on mortgages that consumers would repay. Since these are loans people will repay, the CFPB expects lenders will also benefit from improved underwriting and increased volume of safe loan approvals. In terms of mortgages, the CFPB expects the proposed rule would lead to the approval of approximately 22,000 additional, safe mortgages every year.

In December 2014, the CFPB released a report showing that medical debts provide less predictive value to lenders than other debts on credit reports. Then in March 2022, the CFPB released a report estimating that medical bills made up $88 billion of reported debts on credit reports. In that report, the CFPB announced that it would assess whether credit reports should include data on unpaid medical bills.

Since the March 2022 report, the three nationwide credit reporting conglomerates – Equifax, Experian, and TransUnion – announced that they would take many of those bills off credit reports, and FICO and VantageScore, the two major credit scoring companies, have decreased the degree to which medical bills impact a consumer's score.

Despite these voluntary industry changes, 15 million Americans still have $49 billion in outstanding medical bills in collections appearing in the credit reporting system. The complex nature of medical billing, insurance coverage and reimbursement, and collections means that medical debts that continue to be reported are often inaccurate or inflated. Additionally, the changes by FICO and VantageScore have not eliminated the credit score difference between people with and without medical debt on their credit reports. We expect that Americans with medical debt on their credit reports will see their credit scores rise by 20 points, on average, if the proposed rule is finalized.

Under the current system, debt collectors improperly use the credit reporting system to coerce people to pay debts they may not owe. Many debt collectors engage in a practice known as "debt parking," where they purchase medical debt then place it on credit reports, often without the consumer's knowledge. When consumers apply for credit, they may discover that a medical bill is hindering their ability to get a loan. Consumers may then feel forced to pay the medical bill in order to improve their credit score and be approved for a loan, regardless of the debt's validity.

Specifically, the proposed rule, if finalized would:

Eliminate the special medical debt exception: The proposed rule would remove the exception that broadly permits lenders to obtain and use information about medical debt to make credit eligibility determinations. Lenders would continue to be able to consider medical information related to disability income and similar benefits, as well as medical information relevant to the purpose of the loan, so long as certain conditions are met.

Establish guardrails for credit reporting companies: The proposed rule would prohibit credit reporting companies from including medical debt on credit reports sent to creditors when creditors are prohibited from considering it.

Ban repossession of medical devices: The proposed rule would prohibit lenders from taking medical devices as collateral for a loan, and bans lenders from repossessing medical devices, like wheelchairs or prosthetic limbs, if people are unable to repay the loan.

The CFPB began today's rulemaking in September 2023 with the goals of ending coercive debt collection practices and limiting the role of medical debt in the credit reporting system. The CFPB additionally published in 2022 a report describing the extensive and debilitating effects of medical debt along with a bulletin on the No Surprises Act to remind credit reporting companies and debt collectors of their legal responsibilities under that legislation.

Comment: The CFPB projected the rulemaking in September 2023, and the proposal comes on the heels of several state laws prohibiting inclusion of medical debt information on consumer reports.

Technology / Security

CSBS Strengthening Cybersecurity (06/12/2024) – Working with the Bankers Electronic Crimes Task Force and the United States Secret Service, state supervisors released Ransomware Self-Assessment Tools (R-SAT) for both banks and nonbanks in 2020. R-SAT helps financial institutions assess how they can mitigate ransomware risks and identify other cybersecurity gaps.

In October 2023, they released a new, updated R-SAT for banks to address new risks associated with ransomware attacks and identify security gaps. The updated R-SAT incorporates insights from cybersecurity experts, feedback from financial institutions, and lessons learned from analyzing real-life ransomware attacks.

While financial institutions may have good cybersecurity practices in place, rapid advancements in ransomware techniques and the potentially devastating consequences of a successful attack require every financial institution to review and update their ransomware-specific controls. The updated R-SAT places an increased emphasis on topics such as multi-factor authentication, employee awareness and security training, cloud-based systems or activities, and the identification of control risks that have not been mitigated to an acceptable risk level.

An industry-wide webinar hosted by CSBS briefed bankers on the updated tool, covering the specific changes to the R-SAT, research, and insights from the industry that led to these changes, and how banks can most effectively leverage the tool to protect their institutions and customers. State regulators continue to be proactive and adaptive to the needs of the diverse banking system. Updates to the R-SAT are yet another example of state regulators empowering their institutions with tools to protect our financial system and the customers it serves.

Related Topics: ANNUAL REPORT

Comment: The RSAT 2.0 was first released in October 2023.

🟩	**CISA** JCDC, Government and Industry Partners Conduct AI Tabletop Exercise (06/14/2024) – WASHINGTON – The Cybersecurity and Infrastructure Security Agency (CISA) conducted the federal government's inaugural tabletop exercise with the private sector focused on effective and coordinated responses to artificial intelligence (AI) security incidents. This exercise brought together more than 50 AI experts from government agencies and industry partners at the Microsoft Corp. facility in Reston, Virginia. The four-hour exercise was led by the Joint Cyber Defense Collaborative (JCDC), a public-private partnership model established by CISA to undertake joint planning efforts and drive operational collaboration. This exercise simulated a cybersecurity incident involving an AI-enabled system and participants worked through operational collaboration and information sharing protocols for incident response across the represented organizations. CISA Director Jen Easterly and FBI Cyber Division Deputy Assistant Director Brett Leatherman delivered opening and closing remarks, respectively, emphasizing the need for advancing robust operational structures to address existing and potential security threats, while prioritizing secure-by-design AI development and deployment. This tabletop exercise is supporting the development of an AI Security Incident Collaboration Playbook spearheaded by JCDC.AI, a dedicated planning effort within JCDC focused on building an operational community of AI providers, AI security vendors, and other critical infrastructure owners/operators to address risks, threats, vulnerabilities, and mitigations concerning AI-enabled systems in national critical infrastructure. The playbook, slated for publication by year-end, will facilitate AI security incident response coordination efforts between government, industry, and global partners. “This exercise marks another step in our collective commitment to reducing the risks posed by AI. It also highlights the importance of developing and delivering AI products that are designed with security as the top priority,” said CISA Director Jen Easterly. “As the national coordinator for critical infrastructure security and resilience, we’re excited to work with our partners to build on this effort to help organizations secure their AI systems.” “This exercise demonstrates the FBI’s commitment to leveraging its partnerships to ensure that we are all better prepared to handle threats in this space,” said Assistant Director Bryan Vorndran of the FBI’s Cyber Division. “We are stronger when we come together to share information and determine best practices in the evolving AI landscape. We will continue to work extensively with our interagency and private sector partners to combat bad actors and safeguard infrastructure.” "This gathering shows the value of preparation and collaboration for cyber incident response. As we enter a new AI Landscape, security is critical, and collaboration with industry and government partners is crucial to developing an effective and coordinated response to security incidents. Practicing response scenarios and simulations like the AI-focused tabletop exercise drive learning and sharing that will help strengthen cyber resilience across the board. Security is a top priority at Microsoft, and we appreciate CISA's leadership, as well as the opportunity to host and participate in this exercise,” said Bret Arsenault, CVP, Chief Cybersecurity Advisor, Microsoft. “Palo Alto Networks is proud to partner with the JCDC.AI and other industry partners on this critical exercise. The opportunity to work with other industry-leading AI experts and simulate the compromise of a critical AI system will give us all the ability to enhance response strategies and improve AI security systems to better protect digital ecosystems that rely on AI capabilities. As the adoption of AI has expanded, we’ve seen a similar growth in complexity in the cyber threat environment. Public-private collaborations on critical exercises like this will better protect our digital way of life,” said Sandy Reback, Vice President, Public Policy & Government Affairs, Palo Alto Networks. "The insights we will gain from this exercise will be vital for developing immediate response strategies and shaping the future of AI security. The upcoming AI Security Incident Collaboration Playbook will serve as a

critical resource for all stakeholders, ensuring that we will be prepared and resilient in the face of AI-related threats," said Jonathan Dambrot, CEO of Cranium.

“AI applications are increasingly becoming high-value targets for threat actors, and the current speed at which vulnerabilities are being discovered puts them at an advantage. Coordinated AI threat intelligence sharing and response is critical to helping organizations securely adopt AI and safeguard their systems, and we're pleased to participate in the JCDC tabletop exercise," said Hyrum Anderson, Chief Technology Officer, Robust Intelligence.

"At OpenAI, we firmly believe that security is a team sport. It thrives on collaboration and benefits immensely from transparency. We are proud to have taken part in the tabletop exercise with JCDC.AI and other security leaders—these collaborations benefit our efforts of safely developing and deploying AI technology. This initiative not only strengthens our defenses but also fosters a community dedicated to collective security advancements, which includes realizing the benefits of using AI tools for cyber defense,” said Matt Knight, Head of Security at OpenAI.

"Simulating adversarial threats against AI systems in a controlled setting is an invaluable training ground to equip security teams with an understanding of the vulnerabilities and threats that exist today. Hidden Layer is honored to join this initiative, which underscores our shared dedication to empowering organizations to adopt AI securely while protecting our national infrastructure from emerging threats," said Chris Sestito, CEO & Co-Founder of Hidden Layer.

“With critical infrastructure facing increasingly severe attacks and the rise of AI threats, early preparedness and routine testing is more important than ever to reduce any collateral damage,” said Troy Bettencourt, Global Partner, Head of IBM X-Force. “We are proud to join CISA JCDC and participate in this foundational exercise uncovering the insights and actions needed to help protect these vital organizations from AI-based attacks.”

“At Protect AI we are committed to building a safer AI powered world. This exercise is an important one to ensure that organizations are securing AI commensurate to the value it delivers. We are honored to be a part of it, and will continue to support the ongoing efforts of CISA to ensure that AI is being built and used securely,” said Ian Swanson, Protect AICEO and Co-Founder.

"Scale AI is proud to participate in the JCDC's inaugural AI security tabletop exercise, reinforcing our commitment to secure-by-design principles in AI development. Our collaboration highlights the essential role of public-private partnerships in enhancing the resilience of national critical infrastructure against AI-related threats," said Alex Levinson, Head of Security, Scale AI.

"I applaud CISA's effort on the development of the AI Security Incident Collaboration Playbook, a well-needed initiative spearheaded by JCDC. This tabletop exercise marks a significant step forward in enhancing an operational community of fellow AI providers, AI security vendors, and critical infrastructure owners and operators. This playbook will serve as a great resource for coordinating AI security incidents among industry peers and global partners, ensuring a resilient and secure technological future," said Omar Santos, Security and Trust, Cisco.

Participants included the Amazon Web Services, Cisco, Cranium, Hidden Layer, IBM, Microsoft, NVIDIA, OpenAI, Palantir, Palo Alto Networks, Protect AI, Robust Intelligence, Scale AI, Federal Bureau of Investigation, National Security Agency, Office of the Director for National Intelligence, Department of Defense, and Department of Justice, and other leading technology firms. A second exercise later this year will incorporate AI integrators in U.S. critical infrastructure.

🟩	These efforts align with CISA Roadmap for AI and the 2024 JCDC Priorities, focusing on establishing incident response capabilities and decreasing AI-related threats to national critical infrastructure through robust public-private collaboration. For more information on CISA’s work, visit Artificial Intelligence.

Selected federal rules – proposed

Proposed rules are included only when community banks may want to comment. Date posted may not be the same as the Federal Register Date.