Regulatory Dispatch

Timely news and resources community bankers can use

to better stay on top of a rapidly changing world.

ICBA Releases Guide on Contacting Regulators About Check Fraud

ICBA's Check Fraud Task Force **published a new guide** that explains how and when community banks should contact regulators about check fraud.

Background: Check Fraud: Engagement with Federal Bank Regulators was developed by the community bankers who comprise ICBA's Check Fraud Task Force. It also offers suggestions on how to frame feedback and where to direct communication based on the experiences of peer community bankers.

Contact ICBA: ICBA continues to raise awareness of check fraud in the news media and encourages community bankers to share their experiences and input on the challenge of check fraud at **checkfraud@icba.org**.

More: ICBA this year has also published **Check Fraud: Detection Mechanisms** and **Check Fraud: A Practical Guide to Altered, Forged, and Counterfeit Checks for Community Bankers**.

Other Resources: For more information on check fraud, community bankers can:

- **Join** the fraud subgroup on ICBA Community.
- **Listen** to an Independent Banker podcast on the issue.
- **Read** Independent Banker's latest article on check fraud mitigation tips.
- **Watch** the recording of ICBA's ThinkTECH Solutions Forum on fraud.
- **See** recent media coverage of the issue generated by ICBA.

Comment: Check fraud has seen a meteoric rise over the past three years. According to a report published by FinCEN in 2023, check fraud has more doubled since 2021; reaching a reported 680,000 cases of possible check fraud last year. One of the biggest problems facing community banks is getting the largest bans to honor presentment warranties. These tools help with that problem.

Bank Management

	FRB Speech by Governor Bowman on Artificial Intelligence in the Financial System (10/18/2024) – *First, we must understand AI before we consider whether and how to change our regulatory approach. With respect to various internal use cases, the Board has published a compliance program that governs artificial intelligence.11 One of the foundational elements for a successful approach to AI, and one mentioned in this plan, is the development and acquisition of staff expertise.*

Many banks have increased AI adoption to an expanding number of use cases. As this technology becomes more widely adopted throughout the financial system, it is critical that we have a coherent and rational policy approach. That starts with our ability to understand the technology, including both the algorithms underlying its use and the possible implications—both good and bad—for banks and their customers.

In suggesting that we grow our understanding and staff expertise as a baseline, I acknowledge that this has been, and is likely to remain, a challenge. The Federal Reserve and other banking regulators compete for the same limited pool of talent as private industry. But we must prioritize improving our understanding and capacity as this technology continues to become more widely adopted.

Second, we must have an openness to the adoption of AI. We need to have a receptivity to the use of this technology and know that successful adoption requires communication and transparency between regulated firms and regulators. One approach regulators can use to reframe questions around AI (and innovation generally) is to adopt a posture that I think of as technology agnosticism.

We should avoid fixating on the technology, and instead focus on the risks presented by different use cases. These risks may be influenced by a number of factors, including the scope and consequences of the use case, the underlying data relied on, and the capability of a firm to appropriately manage these risks. Putting activities together may be a helpful way to get a sense of broad trends (for example, the speed of AI adoption in the industry), but is inefficient as a way to address regulatory concerns (like safety and soundness, and financial stability). This may seem like an obvious point, but at times regulators have fallen prey to overbroad categorizations, treating a diverse set of activities as uniformly and equally risky.

This approach allows us to be risk-focused, much like we try to do with other forms of supervision, moderating intensity for low-risk activities, and increasing the intensity for higher-risk ones.

Of course, regulatory agencies do not operate in a vacuum, so we must also ask what type of coordination we need to ensure that we promote safe and sound adoption of AI, and address broader financial stability risks, both domestically and internationally. As a threshold matter, we need coordination both within each agency and among domestic regulators that play a role in the supervision and regulation of the financial system, which requires an environment of open sharing of information.

A posture of openness to AI requires caution when adding to the body of regulation. Specifically, I think we need a gap analysis to determine if there are regulatory gaps or blind spots that could require additional regulation and whether the current framework is fit for purpose. Fundamentally though, the variability in the technology will almost certainly require a degree of flexibility in regulatory approach.

Closing Thoughts

	Before closing, I want to thank the organizers of this event for the invitation to address you this evening, and to thank the many speakers and participants who have contributed to the symposium. *Artificial intelligence has tremendous potential to reshape the financial services industry and the broader world economy. While I have suggested in my remarks that we need not rush to regulate, it is important that we continue to monitor developments in AI and their real-world effects. In the long run, AI has the potential to impact many aspects of the Fed's work, from our role in supervising the payment system, to the important work we do promoting the safe and sound operation of banks and financial stability. AI may also play a growing role in monetary policy discussions, as the introduction of AI tools alter labor markets, affecting productivity and potentially the natural rate of unemployment and the natural rate of interest.* *But as we engage in ongoing monitoring—and expand our understanding of AI technology and how it fits within the bank regulatory framework—I think it is important to preserve the ability of banks to innovate and allow the banking system to realize the benefits of this new technology.* ***Comment: BankDirector.com recently published an interesting article entitled Practical AI Considerations for Community Banks that is worth reading.***
	FRB Approaching Policymaking Pragmatically - Governor Michelle W. Bowman (10/18/2024) – *A Pragmatic Approach to Policymaking A Goal-Oriented Approach* *In the past, I have discussed the role of policymaking from the perspective of a Federal Reserve Board member. But taking a step back, there are some broader themes relevant to agency policymaking more generally, themes that are useful beyond the context of the Federal Reserve. At a basic level, I think of this as a pragmatic approach. It requires tradeoffs to balance regulation while also not inhibiting economic growth.* *The first question I like to ask when confronted with a policy issue is, "Why are we here?" You may recognize this question from Philosophy 101, but this question also applies to the exercise of executive authority by regulatory agencies. The Federal Reserve has extensive responsibilities, and equally extensive powers, but it must exercise these powers only in furtherance of specific goals established by statute. The sheer scope of the Fed's powers can present a temptation to go beyond the statutory authority. For example, to play a more active role in the allocation of credit, or to displace other sources of bank funding even when market sources of liquidity are functioning well. It could also include the temptation to venture into policy matters unrelated to the Fed's responsibilities that are better addressed by Congress or other policymakers (here, a push for banking sector climate change related regulation comes to mind). The goals Congress has laid out for the Fed are complicated and important. Congress should not expect the Federal Reserve, or any other agency for that matter, to solve problems beyond that agency's limited purpose. Doing so would contravene the intent and authority of Congress.*

	To begin, I will provide a few concrete examples of how the starting point for policy is the agency's mission, including in: (1) the execution of monetary policy, and (2) the conduct of banking regulation and supervision.

Deposit / Retail Operations

	CFPB Finalizes Rule on Federal Oversight of Popular Digital Payment Apps to Protect Personal Data, Reduce Fraud, and Stop Illegal "Debanking" (11/21/2024) – The Consumer Financial Protection Bureau (CFPB) finalized a rule to supervise the largest nonbank companies offering digital funds transfer and payment wallet apps. The rule will help the CFPB to ensure that these companies – specifically those handling more than 50 million transactions per year – follow federal law just like large banks, credit unions, and other financial institutions already supervised by the CFPB. The CFPB estimates that the most widely used apps covered by the rule collectively process over 13 billion consumer payment transactions annually. "Digital payments have gone from novelty to necessity and our oversight must reflect this reality," said CFPB Director Rohit Chopra. "The rule will help to protect consumer privacy, guard against fraud, and prevent illegal account closures." Digital payment apps have become a cornerstone of daily commerce, rivaling traditional payment methods like credit cards and debit cards for both online and in-store purchases. Some of these apps are owned by the world's largest technology conglomerates. These services have gained particularly strong adoption among middle and lower-income consumers, who now use payment apps for daily spending and funds transfers at rates that rival or exceed the use of cash. What began as a convenient alternative to cash has evolved into a critical financial tool, processing over a trillion dollars in payments between consumers and their friends, families, and businesses. While banks and credit unions offering consumer payment services are subject to CFPB supervisory examinations, many of these very large technology firms handling billions of transactions are not. The CFPB has closely observed developments in this emerging market, including by monitoring consumer complaints and launching an inquiry into Big Tech and peer-to-peer platforms offering popular payment apps. The final rule will enable to the CFPB to supervise companies in key areas including: ▪ **Privacy and Surveillance:** Large technology companies are collecting vast quantities of data about an individual's transactions. Federal law allows consumers to opt-out of certain data collection and sharing practices, and also prohibits misrepresentations about data protection practices. ▪ **Errors and Fraud:** Under longstanding federal law, consumers have the right to dispute transactions that are incorrect or fraudulent, and financial institutions must take steps to look into them. The CFPB is particularly concerned about how digital payment apps can be used to defraud older adults and active duty servicemembers. Some popular payment apps appear to design their systems to

shift disputes to banks, credit unions, and credit card companies, rather than managing them on their own.

- **Debanking:** Given the volume of payments consumers make through many popular payment apps, consumers can face serious harms when they lose access to their app without notice or when their ability to make or receive payments is disrupted. Consumers have reported concerns to the CFPB about disruptions to their lives due to closures or freezes.

While the CFPB has always had enforcement authority over these companies, the rule gives the CFPB the authority to conduct proactive examinations to ensure companies are complying with the law in these and other areas. Supervision can prevent harm by detecting problems early. Supervision also is an important tool for the CFPB to assess risks that can emerge rapidly in this market, including from outages and other issues that could lead to millions of consumers losing access to their funds.

In the final rule, the CFPB made several significant changes from its initial proposal. The transaction threshold determining which companies require supervision is now substantially higher, at 50 million annual transactions. Given the evolving market for digital currencies, the CFPB also limited the rule's scope to count only transactions conducted in U.S. dollars.

The rule represents the latest step to strengthen oversight of large technology firms in consumer financial markets. The CFPB warned Big Tech firms in 2022 about their obligations under consumer protection laws when using behavioral targeting for financial products. The CFPB also issued a report about how funds held in some popular apps are not protected by federal deposit insurance, and advised consumers to regularly move their funds to an insured account. The CFPB also published research about regulations imposed by Apple and Google in the “tap-to-pay” market.

CFPB Supervision has also created a supervision technology program which assesses, among other things, technology and technology controls and its impact on compliance with Federal consumer financial law.

The final rule is the sixth rulemaking by the CFPB to define larger participants operating in markets for consumer financial products and services. The first five rules covered larger participants in consumer reporting, consumer debt collection, student loan servicing, international money transfers, and automobile financing.

The rule will be effective 30 days after publication in the *Federal Register*.

Read the final rule.

Comment: The rule defines larger participants of a market for general-use digital consumer payment applications, a market that encompasses specific activities. The market definition generally includes nonbank covered persons that provide funds transfer or payment wallet functionalities through a digital payment application for consumers' general use in making consumer payments transactions, which are defined to

	include payments to other persons for personal, household or family purposes, excluding certain transactions.
	ICBA New Podcast on Combating Holiday-Season Fraud (11/19/2024) – The latest **Independent Banker podcast** spotlights how community bankers can get ahead of year-end fraud and raise awareness among consumers as the holidays approach. **Details:** In the latest episode, Visa Global Head of Payment Systems Intelligence Kausar Kenning said the holidays require additional vigilance and proactive efforts because fraudsters are more likely to seek out vulnerable, lonely, or busy people at the end of the year. **More:** Previous **episodes of the podcast** spotlight check fraud, banking schools, fintech partnerships, and more. ***Comment: Find ways to share with your accountholders.***
	FRB New Payments Study Details Card Use in the US (11/18/2024) – This post unpacks some of the findings from the Federal Reserve's recent study on card use in the US. ***Comment: The study includes some interesting charts that compare business and consumer use by card types that could be helpful in degerming your banks card strategy.***
	FRB When Synthetic Identities and Artificial Intelligence Collide (10/18/2024) – Generative artificial intelligence (Gen AI) is now being used to create realistic-seeming synthetic identities faster than ever before. As a result, financial institutions face the potential for increased losses from the malicious use of synthetic accounts. However, many organizations also have found positive uses for the technology to counter synthetic identity fraud. Explore this trend further with a new downloadable resource, ***Generative Artificial Intelligence Increases Synthetic Identity Fraud Threats***, in the Federal Reserve's **Synthetic Identity Fraud Mitigation Toolkit**. ***Comment: This appears to be the growing fraud frontier. Be aware and find ways to be prepared.***

Lending

	CFPB Announces Threshold Adjustments Under TILA (Regulation Z) and FCRA (Regulation V) (11/20/2024) – The CFPB has issued two final rules adjusting thresholds. First, the CFPB has issued a final rule amending the official interpretations for Regulation Z, which implements the Truth in Lending Act (TILA). The CFPB is required to calculate annually the

	dollar amounts for several provisions in Regulation Z. This final rule revises dollar amounts for certain provisions implementing TILA and amendments to TILA impacting HOEPA loans and qualified mortgages. Second, the CFPB has issued the annual adjustment to the maximum amount consumer reporting agencies may charge consumers for making a file disclosure to a consumer under the Fair Credit Reporting Act (FCRA). The ceiling on allowable charges under Section 612(f) of the FCRA will remain unchanged at $15.50, effective for 2025. These adjustments are applicable January 1, 2025, consistent with relevant statutory or regulatory provisions. You can access the TILA notice at: https://www.consumerfinance.gov/policy-compliance/rulemaking/final-rules/truth-lending-regulation-z-annual-threshold-adjustments-card-act-hoepa/. You can access the FCRA notice at: https://www.consumerfinance.gov/policy-compliance/rulemaking/final-rules/fair-credit-reporting-act-disclosures/. ***Comment: Routine annual adjustments. Be sure to update your policies and procedures accordingly.***

Technology / Security

	CISA 2024 CWE Top 25 Most Dangerous Software Weaknesses (11/20/2024) – The Cybersecurity and Infrastructure Security Agency (CISA), in collaboration with the Homeland Security Systems Engineering and Development Institute (HSSEDI), operated by MITRE, has released the 2024 CWE Top 25 Most Dangerous Software Weaknesses. This annual list identifies the most critical software weaknesses that adversaries frequently exploit to compromise systems, steal sensitive data, or disrupt essential services. Organizations are strongly encouraged to review this list and use it to inform their software security strategies. Prioritizing these weaknesses in development and procurement processes helps prevent vulnerabilities at the core of the software lifecycle. Addressing these weaknesses is integral to CISA's **Secure by Design** and **Secure by Demand** initiatives, which advocate for building and procuring secure technology solutions: • **Secure by Design:** Encourages software manufacturers to implement security best practices throughout the design and development phases. By proactively addressing common weaknesses found in the CWE Top 25, manufacturers can deliver inherently secure products that reduce risk to end users. Learn more about Secure by Design here. • **Secure by Demand**: Provides guidelines for organizations to drive security improvements when procuring software. Leveraging the CWE Top 25, customers can establish security expectations and ensure that their software vendors are

committed to mitigating high-risk weaknesses from the outset. Explore how you can integrate Secure by Demand principles here.

Recommendations for Stakeholders:

- **For Developers and Product Teams**: Review the 2024 CWE Top 25 to identify high-priority weaknesses and adopt Secure by Design practices in your development processes.
- **For Security Teams**: Incorporate the CWE Top 25 into your vulnerability management and application security testing practices to assess and mitigate the most critical weaknesses.
- **For Procurement and Risk Managers**: Use the CWE Top 25 as a benchmark when evaluating vendors, and apply Secure by Demand guidelines to ensure that your organization is investing in secure products.

By following CISA's initiatives, organizations can reduce vulnerabilities and strengthen application and infrastructure security. Incorporating the 2024 CWE Top 25 into cybersecurity and procurement strategies will enhance overall resilience.

For further details, refer to the full 2024 CWE Top 25 list here.

Comment: According to cybersecurity authorities, the top threats facing the financial sector today include ransomware, phishing, external-facing application vulnerabilities, and Distributed Denial of Service (DDoS) attacks. As community banks become increasingly reliant on technology service providers to meet customer demands, the need for robust cybersecurity measures is paramount.

CISA and Partners Release Update to BianLian Ransomware Cybersecurity Advisory (11/20/2024) – CISA, the Federal Bureau of Investigation (FBI), and the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) released updates to #StopRansomware: BianLian Ransomware Group on observed tactics, techniques, and procedures (TTPs) and indicators of compromise attributed to data extortion group, BianLian.

The advisory, originally published May 2023, has been updated with additional TTPs obtained through FBI and ASD's ACSC investigations and industry threat intelligence as of June 2024.

BianLian is likely based in Russia, with Russia-based affiliates, and has affected organizations in multiple U.S. critical infrastructure sectors since June 2022. They have also targeted Australian critical infrastructure sectors, professional services, and property development.

CISA and partners encourage infrastructure organizations and small- to medium-sized organizations implement mitigations in this advisory to reduce the likelihood and impact of BianLian and other ransomware incidents. These mitigations align with the Cross-Sector

	Cybersecurity Performance Goals developed by CISA and the National Institute of Standards and Technology. This advisory is part of CISA's ongoing #StopRansomware effort. ***Comment: Reminder that the CSBS updated the original R-SAT to R-SAT 2.0 in October 2023 to further assist banks in the evolving effort to mitigate risks associated with Ransomware attack vectors. It is certainly a best practice - and well worth the time and effort - to complete the RSAT 2.0.***
	CISA Security Updates (11/22/2024) – **Apple Releases Security Updates for Multiple Products** *11/20/2024 01:00 PM EST* Apple released security updates to address vulnerabilities in multiple Apple products. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system. CISA encourages users and administrators to review the following advisories and apply necessary updates: • iOS 18.1.1 and iPadOS 18.1.1 • macOS Sequoia 15.1.1 • iOS 17.7.2 and iPadOS 17.7.2 • visionOS 2.1.1 • Safari 18.1.1

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.

08.08.2024 **FDIC** Request for Information on Deposits SUMMARY: The Federal Deposit Insurance Corporation (FDIC) is soliciting comments from interested parties on deposit data that is not currently reported in the Federal Financial Institutions Examination Council's (FFIEC) Consolidated Reports of Condition and Income (Call Report) or other regulatory reports, including for uninsured deposits. The FDIC seeks information on the characteristics that affect the stability and franchise value of different types of deposits and whether more detailed or more frequent reporting on these characteristics or types of deposits could enhance offsite risk and liquidity monitoring, inform analysis of the benefits and costs associated with additional deposit insurance coverage for certain types of deposits, improve risk sensitivity in deposit insurance pricing, and provide analysts and the general public with accurate and transparent data. **DATES: Comments must be received**

on or before December 6, 2024 (extended by the FDIC from the original October 7, 2024 deadline.)

09.17.2024 **FDIC** Recordkeeping for Custodial Accounts Summary: SUMMARY: The Federal Deposit Insurance Corporation (FDIC) is proposing requirements that would strengthen FDIC-insured depository institutions' (IDI) recordkeeping for custodial deposit accounts with transactional features and preserve beneficial owners' and depositors' entitlement to the protections afforded by Federal deposit insurance. The proposal is intended to promote the FDIC's ability to promptly make deposit insurance determinations and, if necessary, pay deposit insurance claims "as soon as possible" in the event of the failure of an IDI holding custodial accounts with transactional features. The proposed requirements also are expected to result in depositor and consumer protection benefits, such as promoting timely access by consumers to their funds, even in the absence of the failure of an IDI. The requirements described in this document would only apply to IDIs offering custodial accounts with transactional features and that are not specifically exempted as provided in this NPR. **DATES: Comments must be received by the FDIC on or before January 16, 2025 (extended by the FDIC from the original December 2, 2024 deadline.)**