Regulatory Dispatch

Timely news and resources community bankers can use

Payments Dive Judge Vacates Debit Fee Regulations

U.S. District Judge Daniel Traynor ruled Wednesday that the Federal Reserve exceeded its authority more than a decade ago when it put regulations in place on fees bank card issuers can charge retailers and other merchants when consumers swipe debit cards.

"Accordingly, the Court will vacate Regulation II, 76 Fed. Reg. 43,394 (July 20, 2011), because it is contrary to law and was promulgated in excess of the Board's authority," the U.S. District Court for North Dakota said in a judgement issued Thursday.

The case filed initially by the North Dakota Retail Association and the North Dakota Petroleum Marketers Association against the Federal Reserve in April 2021 is part of a long-standing fee battle between banks and card networks on one side, and retailers and other merchants on the other side. While financial institutions that issue the cards, and their card network partners, have pressed for higher fees, merchants have pushed to lower them.

The judge stayed the decision to give the Fed time to appeal the ruling "to prevent interchange transaction fees from becoming a completely unregulated market," the court order said.

Comment: Notably, the decision leans on Loper Bright Enterprises v. Raimondo, which overturned the "Chevron doctrine," eliminating agency deference and opening the door for more litigation.* While *section 235.5(a) of the current rule exempts banks that have consolidated assets of less than $10 billion as of the end of the calendar year preceding the date of the electronic debit transaction for which the interchange fee is charged or received, a lowering of fees no doubt will have a 'trickle down' effect.

Bank Management

	FRB Speech by Vice Chair for Supervision Bowman on the Economic Outlook and Community Banking (08/09/2025) – *Prioritizing Community Banking Issues - Turning back to community banking, I'd like to share some thoughts about how we identify the key issues facing community banks and prioritize them in our regulatory and supervisory reform efforts.* *My approach to prioritizing these issues remains consistent and clear—it starts with outreach. Throughout my time as a member of the Board, I have focused on meeting with and listening to community bankers to better understand the unique challenges they face. What are the most significant threats to their business? How have regulations harmed or improved their ability to operate safely and soundly? How have competitive factors evolved within their communities? How do they see the business of banking evolving with the introduction of new technologies? Engaging with you and other community bankers has been a critical input to informing my views on the current state of bank regulation and supervision, which also shapes my priorities for regulatory and supervisory initiatives.*

As regulators seek to identify problems in the bank regulatory system and craft approaches to address them, it is imperative that we focus on issues that impact community banks. And I am very pleased to announce that the Board will host a conference focused on community banking in Washington, D.C., on October 9th to ensure that our work is fully informed. We will bring together bankers, industry experts, academics, and other stakeholders to discuss and identify matters targeted to support our ongoing work.

We will continue to fully engage and to understand these banks' concerns. And, apart from fraud, which I'll discuss in more detail in a moment, the Federal Reserve has already started looking at elements of the bank regulatory framework unique to community banks. This includes the community bank leverage ratio (CBLR), liquidity sources and regulatory expectations, and rethinking capital options and operations for mutual banks.

The CBLR is a good example of a well-intentioned measure that underachieved in providing regulatory relief. The CBLR is an optional framework that was designed as an alternative to risk-based capital measures for community banks. A community bank that complies with the CBLR is deemed to comply with risk-based capital requirements.3

Statutory limitations on the CBLR restricted the framework to between 8 and 10 percent for qualifying community banks.4 The agencies initially established the CBLR at 9 percent just as I joined the Board in late 2018.5 In rationalizing this setting, the agencies focused primarily on how many banks would be eligible to opt into the framework at their current capital levels and whether it could essentially retain the same high level of capital in the system.

Implicit in this approach seems to be a view that Congress intended the agencies to keep the same overall amount of capital supporting community banks. However, by statute, Congress provided a range, and the low end is double the standard leverage ratio capital requirement of 4 percent. The regulators also retained many of the same restrictive definitions, like the definition of qualifying tier 1 capital with associated exclusions and caps, that apply more generally to the largest institutions. While there were 4,022 community banks as of the first quarter of 2025, only 1,662 had opted into the CBLR.6

Notably, data show that smaller community banks are more likely to have adopted the CBLR framework. About 53 percent of eligible community banks with assets less than $1 billion have opted in, compared to 26 percent of community banks with assets exceeding $1 billion. These smaller community banks play a significant and unique role in the U.S. economy through their support of local businesses, job creation, and investing in their communities.

In my view, it is time to consider modifications to the CBLR framework that make it a more attractive framework and will encourage more banks to adopt it. We should also consider whether it was appropriately designed and calibrated to fulfill the Congressional intent to achieve regulatory relief. For example, reducing the CBLR requirement from 9 percent to 8 percent could not only allow more community banks to adopt the framework but also increase balance sheet capacity for all CBLR firms, facilitating additional support for local economies through lending.

Since the 2023 failure of Silicon Valley Bank, there has been increased scrutiny on the liquidity sources banks use. Some policymakers have expressed skepticism of long-established and reliable sources of liquidity, particularly liquidity provided by the Federal Home Loan Banks. One proposal, which is perhaps a solution in search of a problem, is to push for an expanded use of the discount window. Under this view, regulators (through requirement or supervisory pressure) would require banks to pledge and maintain assets at the discount window. Banks would be expected to use the discount window as a daily liquidity source, even when other, lower-cost liquidity sources are available like FHLB. But this solution seems to have bypassed the threshold question of whether there is a problem. Effective reform efforts require actual identification of a problem and a practical approach relying on an informed view of the business of banking.

Other small bank concerns have persisted for even longer. Mutual banks have existed since the early 1800s but have long faced limited capital options and restrictions on managing capital distributions.7 I have spoken about these issues in detail in the past, so I will not rehash them today. In the past, when regulators prioritized regulatory reform by asset size alone, they neglected critical issues that affect smaller institutions. Our responsibilities as prudential regulators should be broadly focused on banks of all sizes, ensuring relief across the broad range of asset sizes.

What I have discussed so far today is not an exhaustive list of the work underway at the Board and in partnership with the other agencies. On June 23, the Board announced that reputational risk would no longer be considered in the examination process.8 To implement this lasting change, we are updating guidance, examination manuals, handbooks, and other supervisory materials to ensure the durability of this approach, which is a critical step in addressing the problem of de-banking. A few additional initiatives include changes to provide transparency and efficiency in the supervisory process, better defining "safety and soundness," reviewing and updating relevant asset thresholds used in establishing supervisory categories and regulatory requirements, and rationalizing and updating Bank Secrecy Act and anti-money-laundering requirements.

We have reached a point of opportunity for community banks. It is time to build a framework that supports their strength and vitality, recognizing their unique characteristics so they can prosper long into the future.

BSA / AML

FDIC Supervisory Approach Regarding the Use of Pre-Populated Information for Purposes of Customer Identification Program Requirements (08/05/2025) – Summary:
The FDIC is updating its supervisory approach regarding whether an FDIC-supervised institution can use pre-populated customer information for the purpose of opening an account to satisfy Customer Identification Program (CIP) requirements.

Statement of Applicability: The contents of, and material referenced in, this FIL apply to all FDIC-supervised financial institutions.

	Highlights: The CIP rule, 31 C.F.R. § 1020.220, implements Section 326 of the USA PATRIOT Act, which, among other things, requires financial institutions to implement reasonable procedures for verifying the identity of a person seeking to open an account, to the extent reasonable and practicable, and maintain records of the information used to verify a person's identity. The CIP rule requires an institution to collect certain information from a customer opening an account. It is the FDIC's position that the requirement to collect identifying information "from the customer" under the CIP rule does not preclude the use of pre-filled information. A commonly encountered example is the opening of an account electronically where fields in a digital form are automatically pre-populated (or "pre-filled") with a customer's identifying information. Under the FDIC's interpretation, a financial institution could use information from current or prior accounts or relationships involving the bank or its agents, or other sources, such as parent organizations, affiliates, vendors, and other third parties to pre-fill information that is reviewed and submitted by the customer. The FDIC considers such information from the customer for purposes of the CIP rule. When examining an FDIC-supervised institution that collects identifying information from a customer where some or all of the information was pre-populated, FDIC examiners will consider the pre-filled information as from the customer provided that (1) the customer has opportunity and the ability to review, correct, update, and confirm the accuracy of the information, and (2) the institution's processes for opening an account that involves pre-populated information allow the institution to form a reasonable belief as to the identity of its customer and are based on the institution's assessment of the relevant risks, including the risk of fraudulent account opening or takeover. ***Comment: Banks will no doubt be celebrating a landmark announcement because it has the potential to fundamentally improve the digital account opening process for banks and consumers alike. In the FIL, the FDIC has clarified its supervisory approach, signaling that banks can use pre-populated customer information to fulfill Customer Identification Program (CIP) requirements. A bank may use information from current or prior accounts, affiliates, vendors, or other third parties to pre-fill identifying information, as long as the customer reviews and submits the data. The FDIC said such information is considered "from the customer" under the existing CIP rule.***
	FinCEN Issues Notice on the Use of Convertible Virtual Currency Kiosks for Scam Payments and Other Illicit Activity (08/04/2025) – WASHINGTON—The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued a Notice urging financial institutions to be vigilant in identifying and reporting suspicious activity involving convertible virtual currency (CVC) kiosks. While CVC kiosks can be a simple and convenient way for consumers to access CVC, they are also exploited by illicit actors, including scammers. The risk of illicit activity is exacerbated if CVC kiosk operators fail to meet their obligations under the Bank Secrecy Act (BSA).

	"Criminals are relentless in their efforts to steal money from victims, and they've learned to exploit innovative technologies like CVC kiosks," said **FinCEN Director Andrea Gacki**. "The United States is committed to safeguarding the digital asset ecosystem for legitimate businesses and consumers, and financial institutions are a critical partner in that effort. This Notice supports Treasury's continuing mission to counter fraud and other illicit activities." Illicit activity involving CVC kiosks includes fraud, certain types of cybercrime, and drug trafficking organization activity, which are three of FinCEN's Anti-Money Laundering and Countering the Financing of Terrorism National Priorities. Today's Notice provides an overview of typologies associated with illicit activity involving CVC kiosks. In particular, it highlights the rise in scam payments facilitated by CVC kiosks, including tech and customer support scams and bank imposter scams. Some of these scams disproportionately impact older adults. The Notice highlights red flag indicators and reminds financial institutions of their reporting requirements under the BSA. Questions regarding the contents of this advisory should be sent to the FinCEN Regulatory Support Section by submitting an inquiry at www.fincen.gov/contact. **The full Notice is available online at FIN-2025-NTC1**. ***Comment: FinCEN said that the FBI's Internet Crime Complaint Center received nearly 11,000 complaints involving these machines, with victim losses estimated at around $247 million in 2024. The figures represent a 99% and 31% increase, respectively.***

Deposit / Retail Operations

	FTC Data Show a More Than Four-Fold Increase in Reports of Impersonation Scammers Stealing Tens and Even Hundreds of Thousands from Older Adults (08/07/2025) – In 2024, adults 60 and over reported losing millions to scammers pretending to be from trusted government agencies, businesses. New analysis from the Federal Trade Commission shows a more than four-fold increase since 2020 in reports from older adults who say they lost $10,000 or more—sometimes their entire life savings—to scammers who impersonate trusted government agencies or businesses to convince consumers to transfer money to protect it, when in reality the scammers want to steal it. ***Comment: Excerpt: "New analysis from the Federal Trade Commission shows a more than four-fold increase since 2020 in reports from older adults who say they lost $10,000 or more—sometimes their entire life savings—to scammers who impersonate trusted government agencies or businesses to convince consumers to transfer money to protect it, when in reality the scammers want to steal it. The FTC's latest Consumer Protection Data Spotlight shows a huge jump in losses reported by people 60 and over to these types of impersonation scams in the last four years. Most notably, combined losses***

	reported by older adults who lost more than $100,000 increased eight-fold, from $55 million in 2020 to $445 million in 2024. While younger consumers also have reported these scams, older adults were much more likely to report these extraordinarily high losses.
	Troutman Pepper Locke Bipartisan State AGs Urge Congress to Grant Access to Federally Regulated Banking and Financial Services to State-Regulated Cannabis Businesses (08/06/2025) – In July 2025, a bipartisan coalition of 32 state and territorial attorneys general (AG) sent a letter to Congressional leaders urging the passage of the Secure and Fair Enforcement Regulation (SAFER) Banking Act. Their letter emphasizes that the legislation — a long-stalled federal reform — would provide legal clarity and a safe harbor for banks and financial institutions to serve state-licensed cannabis businesses. Such clarity, they argue, is urgently needed to address public safety risks and to improve the states' ability to regulate and tax the booming cannabis industry. The SAFER Banking Act: Legal Clarity for Ancillary Businesses The core impetus behind the SAFER Banking Act lies in the array of problems caused by forcing a multibillion-dollar industry to operate on an almost entirely cash basis. Nearly 75% of Americans now live in a state where cannabis has been legalized in some form, and legal retail cannabis sales in the U.S. reached more than $30 billion in 2024 (up 4.5% from 2023). Yet, because of marijuana's status as a federally controlled substance and associated federal banking restrictions, state-licensed cannabis companies today have limited or no access to traditional banking, resulting in an overwhelmingly cash-based industry. Legitimate cannabis entrepreneurs are often forced to pay employees and vendors in cash, store cash in vaults or off-site, and even pay taxes by hauling bags of currency to government offices. The cash-only mandate therefore not only creates a host of public health and safety concerns, but also undermines regulatory oversight and tax collection. The SAFER Banking Act is designed to shield banks, credit unions, insurers, and other financial service providers from liability for simply providing traditional business services to state-sanctioned cannabis companies. In essence, it would create a "safe harbor" in federal law so that these ancillary businesses cannot be penalized for offering deposit accounts, loans, insurance, payment processing, and other services to legitimate cannabis-related businesses in jurisdictions where cannabis is legal. By providing a clear statutory safe harbor, the SAFER Banking Act aims to integrate state-legal cannabis commerce into the mainstream U.S. financial system. Importantly, the act does not encourage or facilitate the legalization of cannabis at the state or federal levels, and would not mandate cannabis sales in states that have chosen to keep the drug prohibited. The push for cannabis banking reform has been building in Congress for nearly a decade. The original Secure and Fair Enforcement (SAFE) Banking Act was first introduced in the late 2010s and garnered broad bipartisan support, passing the U.S. House of Representatives multiple times (often by large margins) between 2019 and 2021. These earlier bills, however, ultimately stalled in the Senate. In 2023, lawmakers re-tooled and reintroduced the bill in the 118th Congress with some enhancements — rebranding it as

the “SAFER” Banking Act. The extra “R” in the name signifies an added focus on regulation, and reflects additional provisions to extend protections to ancillary services like insurance and payment processors, and to reinforce requirements for financial regulators to serve all legal businesses fairly.

A Broad Bipartisan Coalition: 32 AGs United

One of the most striking aspects of the July 2025 letter is the breadth of its support among the nation’s top state law enforcement officers. Signatories include the AGs of states with established cannabis markets like California, Colorado, Illinois, and Maryland, as well as conservative-leaning states like Georgia, Ohio, Oklahoma, South Dakota, and Utah. This diversity underscores that access to financial services is not a partisan issue.

As their state’s chief legal officers, AGs are charged with upholding the law and protecting public health and safety. Their collective voice sends a powerful message to Congress that the status quo is failing at the state level — creating unsafe conditions and legal ambiguities — and that federal action is urgently needed to reconcile banking laws with state cannabis laws. This is not the first time state officials have sounded the alarm, as state AGs have sent multiple letters over the years urging federal cannabis banking reform. In May 2019, a bipartisan group of 38 AGs urged Congress to pass the original SAFE Banking Act, citing the public safety hazards of a cash-only industry. More recently, in September 2023, 22 state AGs wrote to Congress in support of the SAFER Banking Act as it advanced through the Senate Banking Committee. Such a broad consensus among state law enforcement leaders, from states with and without legal cannabis, highlights that this issue transcends typical political divides. The AGs collectively recognize that, regardless of a state’s stance on legalizing cannabis, refusing legitimate businesses access to banking serves no one — licensed businesses, regulators, law enforcement, or the public.

Why It Matters

For state-licensed cannabis companies, the stakes in this legislative effort could not be higher. These businesses, which now support more than 425,000 American jobs and counting, have been operating at a severe disadvantage by being denied access to basic banking services that other industries take for granted. The lack of access to checking accounts, electronic payments, lines of credit, and financing not only increases operating costs and security risks, but also hampers the industry’s ability to expand as a bona fide part of their state economies. The SAFER Banking Act promises to finally bridge the gap between federal law and the reality in more than 40 states and territories by removing the cloud of illegality from banking transactions with cannabis businesses.

The unified call to action by 32 AGs signals that state law enforcement leaders see this as a critical public safety issue, not a partisan or ideological question. Their letter makes clear that maintaining the status quo “presents a considerable safety issue for the public” and undermines state oversight. In their view, providing a federal safe harbor for cannabis banking is a pragmatic step that will make communities safer and governance more effective, without endorsing or expanding cannabis use in states that haven’t chosen to legalize.

	Comment: With a renewed emphasis on fair banking and removing reputational risk, it seems logical that a bank should be able to provide services to the cannabis industry. The United States Cannabis Market is anticipated to surge from USD 36.94 billion in 2024 to USD 91.10 billion by 2033 and moving away from a cash-based business would allow greater control and security.
	FDIC Consumer News – August 2025 (08/06/2025) – Suggestions for having a plan - Many people think of disaster preparedness as having a stockpile of water, canned food, and flashlights, but you also need access to cash and financial services. That's why it is important to include financial preparedness in your disaster plans. Here is a summary of financial-related suggestions to consider including in your disaster preparedness plan. …snip **Bank availability during a natural disaster** Banks may need to temporarily limit operations because of a natural disaster's impact on a physical bank branch. This might include closing a lobby, converting to drive-thru only services, or encouraging customers to use ATMs or digital channels to access their services. Consider your digital banking options by reading Banking with Third-Party Apps, which was an article in the June 2024 edition of FDIC Consumer News. Also, taking care of simple things like receiving and depositing a check can be overwhelming during a natural disaster. Direct deposit will help you avoid missing out on important income during a disaster. Regardless of the operating conditions, deposits in an account at an FDIC-insured bank or savings institution will continue to be insured in the unlikely event of a bank failure, to at least $250,000 per depositor, per FDIC-insured bank, per ownership category. Please see additional information regarding FDIC deposit insurance.
	FRB New Online Toolkits for Scams and Check Fraud Mitigation (08/05/2025) – **Scams Mitigation Toolkit** A scam is defined as the use of deception or manipulation intended to achieve financial gain. This growing, evolving threat impacts individuals, businesses and entire economies. Consequences include financial, emotional and psychological tolls. In some cases, the stolen money fuels global organized crime. The newly published Scams Mitigation Toolkit includes the following easy-to-navigate modules: Toolkit Module 1: Scam Basics — Explains what scams are, why you should care, and how and why scams occur. Toolkit Module 2: Scam Tactics and Impacts — Provides examples of how criminals fool us using technology (e.g., generative artificial intelligence, malware); force action through fear, threats and other tactics involving emotional manipulation; and use successful scams to perpetrate other types of fraud.

Test Your Knowledge: Can You Spot the Scam? Test your ability to detect scams by reviewing three scenarios.

Toolkit Module 3: Scam Scenarios — The ability to classify scams can help support consistent classification and reporting; assist with better identification of trends; and help improve detection and mitigation.

Test Your Knowledge: Can You Classify These Scam Scenarios? Challenge yourself to accurately classify various types of scam examples using the ScamClassifierSM model, which uses a series of questions to differentiate and classify scams and attempted scams by category and type.

The toolkit also includes recommendations on how industry stakeholders can combat scams, from being both vigilant and skeptical, to understanding the technology and tactics scammers use — which in turn, can help potential victims pause to question unsolicited messages and offers.

Check Fraud Mitigation Toolkit

Check fraud is a financial crime that involves the unauthorized use of a paper or electronic check. Its consequences include financial losses; operational disruptions; and eroding trust in financial institutions due to negative customer experiences and questions about whether fraudulent checks should have been prevented, cases resolved more quickly, or if safer practices by the payments issuer could have resulted in more timely, accurate payments.

The newly published Check Fraud Mitigation Toolkit includes the following easy-to-navigate modules:

Toolkit Module 1: Check Fraud Basics — An overview of check fraud methods, types and schemes (how the fraud is facilitated), all of which are important for prevention, detection, associate training, customer education and awareness.

Toolkit Module 2: Check Fraud Schemes — Check fraud could be the result of authorized party fraud, where the account holder willingly sends or writes a check for the purpose of committing fraud — or unauthorized party fraud, where criminals use stolen checks or account information for their own financial gain.

Toolkit Module 3: Preventing and Detecting Check Fraud — Explore this module to learn about how people, processes and technology can work together to mitigate check fraud; and to become familiar with common practices for preventing and detecting fraudulent checks.

The toolkit also includes recommendations on how industry stakeholders can combat check fraud, starting with understanding potential check vulnerabilities and fraud scenarios. Possibly the most important of all: arming financial institutions' employees, customers and external partners with proactive education and knowledge about check fraud to help prevent, detect and mitigate it.

	Comment: Both the Scams and Check Fraud Toolkits offer excellent training materials for your frontline staff.
	FTC Scammers Are Using Fake Websites in A Twist on Jury Duty Scams (08/04/2025) – Scammers are still pretending to be the police, calling to say you've missed jury duty and need to pay. But in a new twist, some scammers are now telling you to visit a website to enter your personal information — all so they can steal it and your money.

Lending

	FRB Consumer Credit - G.19 (08/07/2025) – June 2025 - Consumer credit increased at a seasonally adjusted annual rate of 2.3 percent during the second quarter. Revolving credit increased at an annual rate of 0.7 percent, while nonrevolving credit increased at an annual rate of 2.9 percent. In June, consumer credit increased at an annual rate of 1.8 percent.
	FRB Senior Loan Officer Opinion Survey on Bank Lending Practices (08/05/2025) – The July 2025 Senior Loan Officer Opinion Survey on Bank Lending Practices (SLOOS) addressed changes in the standards and terms on, and demand for, bank loans to businesses and households over the past three months, which generally correspond to the second quarter of 2025. Regarding loans to businesses over the second quarter, survey respondents reported, on balance, tighter lending standards and weaker demand for commercial and industrial (C&I) loans to firms of all sizes. Furthermore, banks generally reported tighter standards and weaker demand for commercial real estate (CRE) loans. For loans to households, banks reported basically unchanged lending standards and weaker demand for residential mortgage loans, on balance. In addition, banks reported tighter lending standards and stronger demand for home equity lines of credit (HELOCs). For consumer loans, standards tightened for credit card loans and remained basically unchanged for auto and other consumer loans. Meanwhile, demand weakened for credit card and other consumer loans and strengthened for auto loans. The July SLOOS included a set of special questions inquiring about the current level of lending standards relative to the midpoint of the range over which banks' standards have varied since 2005. Banks reported that, on balance, levels of standards are currently on the tighter end of the range for all loan categories. Compared with the July 2024 survey, banks reported easier levels of standards for most loan categories except residential real estate (RRE) loans, for which levels of standards were comparable with July 2024. ***Comment: CRE loans are vital for banks, especially community and regional banks. In May of this year, the St. Louis FRB published a blog entitled Banking Analytics: Commercial Real Estate Loan Growth Slows to 11-Year Low that is worth reading.***

Technology / Security

	CISA Issues ED 25-02: Mitigate Microsoft Exchange Vulnerability (08/07/2025) – CISA issued Emergency Directive (ED) 25-02: Mitigate Microsoft Exchange Vulnerability in response to CVE-2025-53786, a vulnerability in Microsoft Exchange server hybrid deployments. ED 25-02 directs all Federal Civilian Executive Branch (FCEB) agencies with Microsoft Exchange hybrid environments to implement required mitigations by **9:00 AM EDT on Monday, August 11, 2025**. This vulnerability presents significant risk to all organizations operating Microsoft Exchange hybrid-joined configurations that have not yet implemented the April 2025 patch guidance. Although this directive is only for FCEB agencies, CISA strongly encourages all organizations to address this vulnerability. For additional details, see CISA's Alert: Microsoft Releases Guidance on Vulnerability (CVE-2025-53786) in Hybrid Exchange Deployments. ***Comment: XXX***

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.

06.16.2025 **Joint** Request for Information on Potential Actions to Address Payments Fraud
SUMMARY: The Office of the Comptroller of the Currency (OCC), Treasury; the Board of Governors of the Federal Reserve System (Board); and the Federal Deposit Insurance Corporation (FDIC) seek public input on questions related to payments fraud. This request for information (RFI) offers the opportunity for interested stakeholders to identify ways that the OCC, the Federal Reserve System (FRS), and the FDIC could take actions collectively or independently in their varying respective roles to help consumers, businesses, and financial institutions mitigate check, automated clearing house (ACH), wire, and instant payments fraud. **DATES: Comments must be received by September 18, 2025.**