U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

September 18, 2025

Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551
Attention: Ann E. Misback, Secretary

Jennifer M. Jones, Deputy Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429
Attention: Comments RIN 3064-ZA49

Office of the Comptroller of the Currency
Chief Counsel's Office
400 7th Street, SW, Suite 3E-218
Washington, DC 20219
Attention: Comment Processing

Re: Request for Information on Potential Actions to Address Payments Fraud

Dear Ladies and Gentlemen:

The U.S. Chamber of Commerce ("Chamber") Center for Capital Markets Competitiveness submits these comments in response to the joint request for information from the Board of Governors of the Federal Reserve System ("FRB"), the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency ("Agencies") entitled Potential Actions to Address Payments Fraud ("Proposal").[1]

The Chamber is committed to protecting consumers and businesses from fraud and scams. Preserving the integrity of the payment ecosystem is essential to maintaining public trust, ensuring financial stability, and fostering long-term economic growth.

[1] https://www.federalregister.gov/documents/2025/06/20/2025-11280/request-for-information-on-potential-actions-to-address-payments-fraud

Payment fraud and scams, driven by illegal acts perpetrated by bad actors, present an escalating threat to consumers, national security, and the broader economy. These crimes erode trust in financial systems, disrupt legitimate commerce, and impose disproportionate costs on consumers, businesses, and financial institutions. The Chamber strongly supports the Agencies' efforts to develop a strategic and coordinated framework to deter criminal behavior while fostering innovation and efficiency across payment channels.

To effectively combat payments fraud and scams, a unified national strategy is essential. This strategy must mobilize the expertise and resources of banks, payment processors, technology providers, communications platforms, federal/state/local law enforcement, regulators, and consumer advocates. Given the increasing prevalence of criminal activity, there is no single sector that can combat fraud and scams alone. By fostering a cross-sector, whole-of-ecosystem approach, policymakers and stakeholders can strengthen defenses, protect consumers, and preserve trust in the U.S. payments system. Such sustained and structured collaboration will ensure the payments ecosystem stays ahead of evolving threats while maintaining the speed, convenience, and innovation that consumers and businesses expect in the digital economy.

This initiative must remain focused on combating the unlawful actions of bad actors, rather than imposing additional regulatory burdens or liability on the financial sector, who are heavily invested in helping consumers protect themselves and their investments. Financial institutions, on behalf of their customers and consumers nationwide, are actively engaged in efforts to protect the integrity of the payment ecosystem. A successful framework must prioritize enforcement against criminals and support wholistic collaborative solutions that strengthen defenses earlier in the chain of illicit activity, before harmful consumer financial transactions may even occur.

It is also critical to recognize the growing national security threat posed by transnational criminal organizations, which necessitates a comprehensive federal response to prevent fraud and scams. The complexity and scale of these challenges demand decisive action and innovation from companies, alongside coordinated government support and law enforcement interventions to reach across borders and dismantle these criminal networks.

In 2024 alone, U.S. consumers reported $12.5 billion in fraud losses — a staggering 25% increase from the prior year.[2] The share of consumers reporting financial losses to scams rose from 27% in 2023 to 38% in 2024.[3] Globally, digital payment fraud is projected to reach $50 billion by the end of the year, with one in every 120 online transactions suspected to be fraudulent.[4] Emerging markets have experienced an 80% surge in peer-to-peer payments fraud, underscoring acute vulnerabilities in rapidly expanding payments channels.[5] These alarming trends underscore the urgent need for swift, coordinated, and decisive intervention to safeguard the resilience of the U.S. payments system and economy.

Within this context, it is important to articulate the distinction between fraud and scams to develop targeted solutions. Unauthorized fraud involves transactions not initiated by the customer, typically addressed through controls like login verification and biometrics, and covered under Regulation E for electronic funds transfers with clear liability and resolution processes. In contrast, authorized payment scams occur when consumers authorize the transfers of funds to scammers but claims they were tricked or deceived by the criminal into allowing the transaction. Addressing these scams requires banks to verify both identity and intent, a complex task where even extensive customer warnings and education will often fall short -- the consumer owns the assets in the account and is entitled to initiate the transaction.

The following responses address specific questions posed in the Proposal to support the Agencies' efforts to create a strategic, coordinated framework that deters criminal activity while also promoting innovation and efficiency throughout the payments ecosystem. Through, tangible and actionable steps, the agencies can enhance collaboration, improve education, and refine regulatory frameworks to mitigate payments fraud effectively.

External Collaboration (RFI Question #1)

What actions could increase collaboration among stakeholders to address payments fraud?

---

[2] https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024
[3] Id.
[4] https://coinlaw.io/digital-payment-fraud-statistics/
[5] Id.

To effectively address payments fraud, increased collaboration among stakeholders is essential. One critical step is the establishment of formalized working groups. These groups should consist of representatives from across industries, including banks, payment processors, technology providers, and regulators. By creating standing joint task forces with clearly defined charters, shared metrics, and regular reporting mechanisms, stakeholders can work together to identify and address emerging threats in a structured and coordinated manner.

Second, secure, privacy-compliant data-sharing protocols should be developed. Real-time sharing of fraud indicators and emerging threat intelligence is vital to staying ahead of bad actors. To encourage participation, it is important to implement necessary safe harbors that protect stakeholders from liability when sharing information in good faith. Such protocols will enable stakeholders to act swiftly and decisively in response to fraud threats.

Third, coordinated awareness campaigns are essential to ensure consistent messaging across the payment ecosystem. Synchronizing outreach efforts between industry and regulatory bodies will help avoid fragmented or conflicting messages, which can undermine efforts to combat fraud. These campaigns should evolve to address changing criminal tactics and ensure that both consumers and businesses are equipped with the knowledge to protect themselves.

Finally, shared incident response frameworks are critical for enabling coordinated responses to large-scale or fast-moving fraud events. By establishing clear protocols for cross-institution collaboration during incidents, stakeholders can minimize the impact of fraud and ensure a swift recovery. These frameworks should include predefined roles, responsibilities, and communication channels to facilitate effective and timely responses.

By implementing these measures, stakeholders can foster a collaborative environment that strengthens defenses against payments fraud and enhances the resilience of the U.S. payments system.

External Collaboration (RFI Question #2)

What types of collaboration, including standard setting, could be most effective in addressing payments fraud? What are some of the biggest obstacles to these types of collaboration?

Standard-setting initiatives, such as expanding FraudClassifierSM and ScamClassifierSM, as well as use of transaction tagging with attributes like purpose of payment, industry of the sender, etc. can address new fraud vectors. Interoperable technology standards, including common APIs and authentication protocols, will enhance collaboration. Strengthening multi-sectoral Information Sharing and Analysis Centers (ISACs) will improve threat intelligence sharing. However, obstacles such as legal liability concerns, competitive sensitivities, resource disparities, and inconsistent terminology must be addressed to foster effective collaboration.

External Collaboration (RFI Question #3)

Which organizations outside of the payments or banking industry might provide additional insights related to payments fraud and be effective collaborators in detecting, preventing, and mitigating payments fraud?

Collaboration with organizations outside the payments and banking industry is essential to combating payment fraud. The technology and telecom sectors can help secure communication channels, while e-commerce platforms and marketplaces can better address fraud in merchant and peer-to-peer channels. Social media and advertising platforms can enhance and facilitate the early detection and takedown of fraudulent campaigns. Consumer advocacy groups can amplify outreach and educate consumers on fraud prevention. Law enforcement and cybersecurity firms provide investigative expertise and threat intelligence. Leveraging the unique capabilities of these sectors will enhance the resilience of the payments ecosystem and protect consumers. Combatting fraud must be an all-in approach.

External Collaboration (RFI Question #4)

Could increased collaboration among Federal and State agencies help detect, prevent, and mitigate payments fraud? If so, how?

Increased collaboration among Federal and State agencies is critical to detecting, preventing, and mitigating payments fraud. Joint enforcement strategies

should be prioritized to coordinate investigations, share case data, and align remedies across jurisdictions. This unified approach will enhance the ability to identify and disrupt fraudulent schemes more effectively.

Harmonized regulations and guidance are also essential to reduce regulatory fragmentation, which fraudsters often exploit. By aligning rules and policies, agencies can close gaps that bad actors use to their advantage, creating a more cohesive and robust defense against fraud.

Centralized reporting mechanisms should be established to create a unified intake and referral system for fraud complaints that is accessible to all agencies. This system would support consumers and industry, by streamlining the reporting process, improving data sharing, and ensuring timely responses to fraud incidents.

Cross-training initiatives are necessary to foster mutual understanding of jurisdictional roles, tools, and best practices among Federal and State agencies. This will enhance collaboration and ensure that all stakeholders are equipped to address the complexities of payments fraud.

Additionally, the creation of a dedicated FBI and DOJ unit exclusively focused on addressing payment fraud and scams would provide the specialized expertise and resources needed to combat these crimes effectively. To support these efforts, it is imperative to increase resources for law enforcement. Without adequate funding and expertise, coordination, including with other law enforcement agencies, and timely detection will continue to face significant challenges.

By addressing these areas, Federal and State agencies can work together to strengthen the resilience of the payments ecosystem and protect consumers and businesses from fraud.

Consumer, Business, and Industry Education (RFI Question #5)

> *In general, what types of payments fraud education are most effective, and why? Would different audiences (for example, industry and consumers) benefit from different types of payments fraud education?*

Effective payments fraud education is essential to safeguarding consumers, businesses, and the broader financial ecosystem. Role- and scenario-based training, such as interactive simulations of real-world threats like business email compromise or account takeovers, can be highly effective. These exercises align with specific job roles and consumer contexts, equipping individuals with practical skills to identify and respond to fraud attempts.

Just-in-time education provides contextual “nudges” at critical moments, such as confirmation prompts, risk flags, or hold-to-confirm mechanisms during payment processes. These interventions can interrupt social engineering tactics and encourage users to pause and verify the legitimacy of transactions.

Tabletop exercises and playbooks are valuable tools for institutions, enabling cross-functional teams to practice fraud detection, escalation protocols, and customer communication strategies. These drills ensure that organizations are prepared to respond swiftly and effectively to fraud incidents.

Microlearning and periodic refreshers are also critical. Short, adaptable modules that address emerging fraud patterns help maintain vigilance without overwhelming participants. This approach ensures that education remains relevant and engaging over time.

Channel-integrated messaging, such as in-app banners, SMS or email security tips, and authenticated notifications, can deliver timely and actionable advice directly within the platforms where payments occur. This integration ensures that users receive guidance when they need it most.

Tailored messaging is crucial for different audiences. Consumers benefit from plain-language stories, checklists, and practical tips, while businesses require education on control testing, approvals hygiene, and vendor validation. The industry, on the other hand, needs access to threat intelligence and coordinated response procedures. Meeting people where they are—whether through print, online resources, or other mediums—ensures that education is accessible and impactful for all stakeholders.

By implementing these targeted and differentiated educational strategies, stakeholders can enhance awareness, reduce vulnerabilities, and build a more resilient payments ecosystem.

Consumer, Business, and Industry Education (RFI Question #6)

Would additional education informing consumers and businesses about safe payment practices be helpful to reduce payments fraud and promote access to safe, secure payment options?

Additional education informing consumers and businesses about safe payment practices would be highly beneficial in reducing payments fraud and promoting access to secure payment options. Targeted education can significantly mitigate authorized fraud and user errors by clarifying higher-risk behaviors and promoting the safe use of faster payment systems. By addressing specific vulnerabilities, such education empowers users to make informed decisions and avoid common pitfalls.

Clear guidance on recourse options, dispute pathways, and authentication processes is essential to building trust in digital payments. When consumers and businesses understand how to resolve issues and protect their transactions, confidence in adopting and utilizing secure payments systems increases, fostering broader participation in the digital economy.

Consistency in messaging across regulators, payment networks, and industry stakeholders is also critical. Unified and clear communication prevents mixed signals that can confuse users and undermine efforts to change behaviors. A cohesive approach ensures that all parties receive the same guidance, reinforcing safe payment practices.

Educational efforts should be designed to reach all consumers. Multilingual, mobile-first materials and partnerships with community organizations can help reach underserved consumers and microbusinesses, ensuring that all users have access to the resources and knowledge needed to navigate the payments ecosystem safely. Education should also be intergenerational starting in elementary schools as our young people use technology at an increasingly earlier age and can be victims of extortion or investment scams. Information efforts must also help our elders be more

aware and avoid scams. By addressing these areas, stakeholders can enhance trust, expand access, and reduce fraud across the payment landscape.

Consumer, Business, and Industry Education (RFI Question #7)

Which approaches could make existing payments fraud education more effective? For example, would targeting outreach to particular audiences or conducting additional education in collaboration with other key stakeholders be effective?

To make existing payments fraud education more effective, targeted outreach to specific audiences is essential. Segmenting audiences by risk profile, such as seniors, new-to-digital users, or small and medium-sized enterprises (SMEs) with remote accounts payable and receivable operations, allows for the delivery of tailored content that addresses their unique vulnerabilities. This approach ensures that education is relevant and actionable for each group.

Collaborating with key stakeholders through co-branded campaigns can significantly enhance the reach and credibility of educational efforts. Partnerships with financial institutions, platforms, telecom providers, employers, schools, and community organizations can amplify messaging and ensure it resonates with diverse audiences.

Providing standardized toolkits is another effective strategy. These toolkits can include plug-and-play checklists, templates, and scripts for processes such as onboarding, vendor changes, and payment verification. Such resources simplify the implementation of best practices and make fraud prevention more accessible to businesses and consumers. Federal agencies, non-profits, and private industry have all developed various versions of toolkits and thus expert collaboration would generate the most effective messages and delivery methods.

Regularly updating educational content using anonymized trend data ensures that materials remain current and relevant. Publishing “what’s new” briefs on emerging scams and refreshing content on a set cadence helps stakeholders stay ahead of evolving threats.

Measurement and testing are critical to refining educational initiatives. Using tools like A/B testing, pre- and post-assessments, and incident trend tracking allows stakeholders to evaluate the effectiveness of their efforts and make data-driven improvements.

Finally, supportive policy levers can encourage broader participation in educational outreach. Offering safe-harbor protections for good-faith educational efforts and fostering information sharing without liability concerns can create an environment where stakeholders feel empowered to collaborate and innovate. By implementing these approaches, payments fraud education can become more impactful and adaptive to the needs of a dynamic and diverse audience.

Consumer, Business, and Industry Education (RFI Question #8)

Are current online resources effective in providing education on payments fraud? If not, how could they be improved?

Current online resources for payments fraud education are often fragmented, using inconsistent terminology and presenting information in a text-heavy, jargon-laden format. These gaps make it challenging for consumers and businesses to access clear, actionable guidance. To address these shortcomings, a unified, regulator-endorsed portal should be created. This hub would harmonize definitions, provide role-based pathways, and offer downloadable assets, ensuring that all users can easily find the information they need.

Interactive tools should also be incorporated to enhance user engagement and understanding. Features such as self-assessments, step-by-step recovery guides, vendor-change verification checklists, and dispute or recourse flow maps can provide practical, hands-on support for individuals and businesses navigating fraud-related challenges.

Embedding educational resources within existing platforms can further improve accessibility. By providing APIs or embeddable widgets, banks, fintech companies, and employers can integrate guidance directly into their own channels, ensuring that users encounter relevant information at critical moments.

Accessibility must be a priority in the design of these resources. A mobile-first user experience, multilingual support, ADA compliance, and plain-language content with visuals and short videos can make the materials more inclusive and user-friendly for diverse audiences.

Finally, timely alerts on emerging scam patterns should be offered through opt-in advisories. These alerts can include shareable, co-brandable content to enable rapid amplification across networks. By addressing these areas, online resources can become more effective in educating users and equipping them to combat payments fraud.

Regulation and Supervision (RFI Question #9)

What potential changes to regulations (apart from the Board's Regulation CC, discussed separately below) could address payments fraud and mitigate the harms from payments fraud to consumers, businesses, and supervised institutions?

To address payments fraud and mitigate its harms to consumers, businesses, and supervised institutions, regulatory changes should focus on strengthening information sharing. Coordination with relevant agencies to expand safe harbors for timely, privacy-compliant fraud intelligence sharing across institutions and sectors is essential. This includes establishing clear authority for cross-sector fraud intelligence sharing, improving consistency in fraud data collection, and ensuring legal protections for institutions acting in good faith to protect consumers and the payments system from fraud.

Authentication and verification standards should also be enhanced to establish baseline expectations for layered authentication and confirmation-of-payee style verification on irrevocable payment rails. Leveraging advanced technologies, such as AI-driven behavioral anomaly detection and biometrics, can further bolster security measures and reduce vulnerabilities in the payment ecosystem.

Modernizing third-party risk management is another critical area for regulatory improvement. Vendor risk expectations for real-time payments should be updated to include model transparency, rigorous testing, and shared utilities for smaller banks.

Regulation and Supervision (RFI Question #10-11)

> *The Board, FDIC, and OCC have issued supervisory guidance on numerous topics that relate to payments fraud detection, prevention, and mitigation.*[14] *Is existing supervisory guidance related to payments fraud sufficient and clear? If not, what new or revised supervisory guidance should the Board, FDIC, and OCC consider issuing on this topic within the respective authorities?*
>
> *How might new or revised supervisory guidance assist small community banks in detecting, preventing, and mitigating payments fraud?*

To enhance the detection, prevention, and mitigation of payments fraud, the Board, FDIC, and OCC should consider issuing new or revised supervisory guidance that consolidates and modernizes existing frameworks. A harmonized, plain-language compendium mapping current guidance to key fraud typologies and controls would provide clarity and consistency for financial institutions. This effort should include modernizing regulatory definitions and authorities to allow banks the flexibility to adopt a risk-based approach for addressing both existing and emerging fraud schemes and scams in the digital payments landscape. For example, banks need the discretion to intervene when suspicion of fraud or scam arises, allowing for transaction and account holds where reasonable, necessitating clarifying requirements across overlapping rules like Regulation CC and the Unified Commercial Code.

Supervisory guidance should also clarify expectations for deploying vendor and AI-based fraud tools, particularly for community banks. Proportional validation requirements for these tools would ensure that smaller institutions can effectively leverage advanced technologies without facing undue compliance burdens. This would enable community banks to adopt innovative solutions tailored to their specific needs and resources.

Additionally, the agencies should develop real-time payments playbooks that provide practical examples for managing faster payments. These playbooks could include pre-transaction warnings, post-incident response protocols, and customer communication strategies. Such guidance would help financial institutions navigate

the complexities of real-time payments while maintaining robust fraud prevention measures.

Metrics and testing practices should also be recommended to improve the effectiveness of consumer and small-to-medium enterprise (SME) education. Outcome metrics, such as social-engineering loss rates, and A/B testing practices can help institutions refine their educational initiatives and better protect their customers from fraud.

Finally, to support small community banks, the agencies should offer exam flexibility for shared services, template policies, and reference architectures. Highlighting acceptable reliance on consortium utilities would further enable these institutions to enhance their fraud prevention capabilities without incurring excessive costs. By implementing these measures, supervisory guidance can become a more effective tool in combating payments fraud and supporting the resilience of the financial ecosystem.

Regulation and Supervision (RFI Question #12)

What is the experience of consumers and businesses when supervised institutions place holds on depositors' funds because of suspected payments fraud? (Regulation CC's "reasonable cause to doubt collectability" exception is discussed separately below.)

To improve the experience of consumers and businesses when supervised institutions place holds on depositors' funds due to suspected payments fraud, transparency standards should be established. These standards would define standardized, non-SAR-breaching reason codes, expected timelines, and escalation paths that can be shared with customers. Providing clear and consistent information would help customers understand the reasons for holds and the steps involved in resolving them.

Service level expectations should also be encouraged to ensure timely responses to customer inquiries. Clear service level agreements (SLAs) are particularly important for cases involving payroll or essential living expenses, where delays can have significant impacts. Timely communication and resolution are critical to maintaining trust and minimizing disruptions for consumers and businesses.

Proportional holds should be promoted to ensure that the duration and scope of holds are limited and based on documented risk assessments. Banks should be enabled to apply item-level and account-level holds when fraud or scam activity is suspected, with periodic reassessments to ensure appropriateness. Safe harbors for good-faith actions would further support institutions in taking necessary steps to protect consumers while avoiding undue burdens.

SAR confidentiality requirements do not prohibit financial institutions from disclosures about held funds or account activity, they only prohibit disclosure of a SAR filing or information indicating whether or not a SAR has been filed to customers and other parties. Rather than seeking to clarify SAR confidentiality rules, it would be much more helpful to focus on privacy requirements which are the more relevant hurdle banks face when potential scam or fraud victims need information about activity in accounts where they've sent funds. Still, enhancing the feedback loop from law enforcement on SARs filed can help institutions refine their fraud prevention programs and better serve their customers.

Finally, institutions should be encouraged to provide recovery guides, dispute pathways, and temporary hardship accommodations where appropriate. These resources can help consumers and businesses navigate the challenges associated with fraud-related holds. Supporting the use of transaction and account holds, when reasonable, ensures that consumers are protected while maintaining access to essential financial services. By implementing these measures, the experience of consumers and businesses can be significantly improved, fostering trust and resilience in the financial system.

Regulation and Supervision (RFI Question #13)

> *The Board, FDIC, and OCC have received complaints from supervised institutions regarding challenges in resolving disputes about liability for allegedly fraudulent checks. What is the experience of supervised institutions when trying to resolve these types of interbank disputes regarding allegedly fraudulent checks? Do these types of interbank disputes arise more frequently in connection with certain types of checks or parties? What actions could the Board, FDIC, and OCC consider, including potential amendments by the Board to Regulation CC, that could improve supervised*

institutions' ability to resolve interbank disputes over liability for allegedly fraudulent checks?

To address the challenges supervised institutions face in resolving disputes about liability for allegedly fraudulent checks, standardized dispute packages should be established. These packages would include required evidence artifacts, data fields, and documentation checklists to reduce unnecessary back-and-forth. Banking agencies should collaborate with banks and trade groups to develop appropriate check fraud-related definitions to codify in Regulation CC, ensuring consistency across jurisdictions. This approach would streamline the resolution process and provide clarity for all parties involved.

Defined timelines and forums are also essential for resolving interbank disputes. Clear response windows and neutral facilitation or recognized arbitration mechanisms should be implemented for persistent disputes. Streamlining resolution procedures for interbank breach of warranty claims would allow these issues to be handled outside of litigation, reducing delays and costs for financial institutions.

Liability clarity is another critical area for improvement. Warranties, alteration versus forgery presumptions, and responsibilities in remote deposit capture and image quality scenarios should be clearly defined. Addressing ambiguities in liability allocation would improve the resolution of interbank check disputes and provide greater certainty for all parties.

To combat repeat offenders, controls should be established to flag recurrent fraud patterns and counterparties. Structured escalation processes and information sharing would enable institutions to detect and disrupt fraud more effectively. Supporting fraud intelligence sharing across institutions and industries would further enhance these efforts.

Digital traceability should also be encouraged to speed up attribution and resolution. The use of image forensics and metadata standards, along with network visibility, would provide participants with actionable risk insights and standardized fraud reporting. These measures would improve the efficiency and effectiveness of resolving interbank disputes, fostering a more resilient and secure financial ecosystem.

Regulation and Supervision (RFI Question #14-15)

> *Regulation CC seeks to balance prompt funds availability with the risk of checks being returned unpaid for reasons that include fraud. What potential amendments to Regulation CC would support timely access to funds from check deposits while providing depository institutions with sufficient time to identify suspected payments fraud?*
>
> *Regulation CC provides six exceptions that allow depository institutions to extend deposit hold periods for certain types of deposits, including deposits for which the depository institution has reasonable cause to doubt the collectability of a check.[18] Is this exception effective in allowing depository institutions to mitigate check fraud while also allowing timely access to funds? Would depository institutions benefit from further clarification on when it may be appropriate to invoke this exception? What are the experiences of businesses and consumers when depository institutions invoke this exception in order to delay the availability of depositors' funds?*

To support timely access to funds from check deposits while providing depository institutions with sufficient time to identify suspected payments fraud, Regulation CC should adopt a risk-based availability approach. This would involve tiered availability timelines that shorten for low-risk items while preserving flexibility for elevated-risk deposits. For example, extending funds availability timelines for cashier's checks, certified checks, teller checks, and government checks to second-day availability would balance the need for fraud prevention with consumer access to funds.

Modern detection capabilities should also be acknowledged in Regulation CC. Where feasible, certain deadlines could be converted to real-time or hour-based standards to improve clarity and efficiency. Additionally, supporting the use of positive pay with payee name verification services would help protect financial institutions from releasing funds in error, further enhancing fraud prevention efforts.

The definition of "expeditious" should be refined to include practical cutoffs, weekend and holiday treatment, and safe harbors for good-faith automated detection. Revising the exception for "new accounts" to better align with current risk trends

would also improve the regulation's effectiveness in addressing fraud while maintaining fairness for consumers and businesses.

Clarifying the reasonable cause exception is another critical step. Providing concrete examples, documentation standards, and standard reason codes would guide consistent application of this exception. Currently, the lack of clarity in the "reasonable cause to doubt collectability" exception limits its ability to mitigate payments fraud and address high-risk deposit patterns effectively.

To mitigate customer impacts, Regulation CC should encourage limits on serial holds, periodic reviews, and clear notices to consumers. Expedited release of non-risk portions of deposits, where possible, would help maintain customer trust and minimize disruptions. Additionally, providing banks with a safe harbor from regulatory actions when restricting accounts or holding items to protect consumers from fraud or scams would support institutions in their efforts to safeguard the payment ecosystem.

Finally, measurement and feedback mechanisms should be implemented to track hold usage, false-positive rates, and customer outcomes. Engaging with the industry to develop safe, consistent, and practical guidelines would ensure that Regulation CC strikes the right balance between fraud prevention and timely access to funds. These measures would enhance the regulation's effectiveness while addressing the needs of both financial institutions and their customers.

Payments Fraud Data Collection and Information Sharing (RFI Question #16)

Broadly, how could payments fraud data collection and information sharing be improved?

To improve payments fraud data collection and information sharing, a standardized, regulator-endorsed reporting framework should be developed. This framework should be adaptable to all payment rails, ensuring consistency and clarity in how fraud data is reported and analyzed. Such a framework would provide a unified approach to capturing and sharing critical information, enabling stakeholders to better understand and address fraud trends.

Incentivizing the consistent capture of key data elements both before a transaction is sent and after fraud is discovered is also essential. Before a transaction is sent it is valuable to 'tag the transaction' with data such as purpose of payment, type of sender, etc., to allow the receiver to conduct a risk assessment. When fraud is

discovered, elements shared should include details such as the type of fraud, the channel through which it occurred, the dollar amount involved, the type of victim, and the modus operandi. By standardizing the collection of this information, stakeholders can gain deeper insights into fraud patterns and develop more effective prevention strategies.

Encouraging real-time or near real-time data exchange for emerging threats via secure platforms is another critical step. Timely sharing of fraud data allows stakeholders to respond quickly to new threats, minimizing their impact and preventing further harm. Secure platforms for data exchange would ensure that sensitive information is protected while enabling rapid collaboration.

Finally, fostering cross-sector integration is vital for achieving broader visibility into fraud patterns. Collaboration among banks, fintech companies, telecom providers, social media, messaging and e-commerce platforms can provide a more comprehensive view of fraud activities across different sectors. This integration would enhance the ability of stakeholders to detect and mitigate fraud, ultimately strengthening the resilience of the payment ecosystem. By implementing these measures, payments fraud data collection and information sharing can be significantly improved, benefiting consumers, businesses, and the broader financial system.

Payments Fraud Data Collection and Information Sharing (RFI Question #17)

> *What barriers limit the collection and sharing of payments fraud data between industry stakeholders, and how could these barriers be alleviated? For example, have specific barriers limited development of solutions or participation in bilaterial or multilateral payments fraud data collection and information sharing? What changes would address these barriers?*

To address the barriers limiting the collection and sharing of payments fraud data between industry stakeholders, several key steps should be taken. Legal and liability risks are a significant concern, and expanding safe harbors and standardizing non-disclosure agreements for fraud intelligence sharing would encourage greater participation. These measures would provide stakeholders with the confidence to share critical information without fear of legal repercussions.

Data privacy concerns also present a challenge. Applying strong anonymization and aggregation protocols can help protect sensitive information while enabling the sharing of valuable fraud data. These protocols would ensure that privacy is maintained while still allowing stakeholders to collaborate effectively.

Cost and resource constraints, particularly for smaller institutions, must also be addressed. Creating shared utilities or subsidized participation models would enable smaller organizations to contribute to and benefit from fraud data sharing initiatives. This approach would ensure that all stakeholders, regardless of size, can participate in efforts to combat payments fraud.

A lack of trust and coordination among stakeholders can further hinder collaboration. Using neutral conveners, such as the FRB, to manage collaborative platforms would foster trust and encourage participation. These conveners could provide a centralized and impartial forum for stakeholders to share information and develop solutions.

Consistency and uniformity in fraud taxonomy are essential for identifying and sharing indicators and trends. Developing a standardized taxonomy in collaboration with industry stakeholders would improve the clarity and effectiveness of fraud data sharing. Additionally, consolidating fraud reporting portals would streamline the process and reduce fragmentation, making it easier for stakeholders to report and access critical information.

By addressing these barriers, the collection and sharing of payments fraud data can be significantly improved, enabling stakeholders to better detect, prevent, and mitigate fraud. These efforts would strengthen the resilience of the payments ecosystem and protect consumers and businesses from evolving threats.

Payments Fraud Data Collection and Information Sharing (RFI Question #18)

> *What role should the FRS, FDIC, or OCC take in supporting further standardization of payments fraud data? For instance, can the FRS better leverage or improve the FraudClassifier℠ and ScamClassifier℠ models?*

The Agencies should play a leading role in supporting the further standardization of payments fraud data. One critical step would be to maintain and enhance the FraudClassifierSM and ScamClassifierSM models to ensure they keep pace with evolving fraud schemes. As fraud tactics become increasingly sophisticated, these models must be regularly updated to reflect new threats and provide financial institutions with the tools needed to identify and mitigate risks effectively.

Additionally, the Agencies should provide implementation guidance and integration toolkits to facilitate consistent adoption of these models across institutions of all sizes. Smaller institutions, in particular, may lack the resources to independently implement these tools, and clear guidance would ensure that all stakeholders can benefit from standardized fraud classification systems. This consistency would enhance the overall effectiveness of fraud prevention efforts across the financial ecosystem.

The FRB should also leverage aggregated reporting to publish anonymized industry benchmarks and trend analyses. By sharing insights derived from fraud data, the FRB can help institutions better understand emerging threats and benchmark their performance against industry standards. These analyses would provide valuable context for financial institutions, enabling them to refine their fraud prevention strategies and stay ahead of evolving risks. By taking these steps, the Agencies can strengthen the standardization of payments fraud data and enhance the resilience of the financial system.

Payments Fraud Data Collection and Information Sharing (RFI Question #19)

What types of payments fraud data, if available, would have the largest impact on addressing payments fraud? If these data are not currently being collected or shared, what entities are best positioned to collect and share such data?

To effectively address payments fraud, certain types of data, if available before and after the payment transaction, would have the largest impact. Before the transaction, data regarding the purpose of payment and the ultimate use case are critical to contextualize the payment and use it in fraud assessment to prevent fraud. Once fraud has been identified, one critical data set is cross-rail repeat offender patterns, which include information on fraudulent accounts and mule networks. Identifying these patterns across payment rails would enable stakeholders to detect and disrupt organized fraud schemes more effectively, reducing the overall impact of such activities on the payment ecosystem.

Another valuable data set is loss attribution by vector, which categorizes fraud incidents based on methods such as social engineering, malware, and account takeover. Understanding the specific vectors through which fraud occurs would allow stakeholders to tailor their prevention and detection strategies to address the most prevalent and damaging methods.

Speed and scale metrics, such as the time from fraud initiation to detection, are also essential. These metrics provide insights into how quickly fraud is identified and the scale at which it occurs, enabling stakeholders to refine their detection systems and improve response times to minimize losses.

Recovery outcomes, including the amounts recovered and the time to resolution, are another important data set. Tracking these outcomes would help stakeholders evaluate the effectiveness of their recovery efforts and identify areas for improvement in mitigating the financial impact of fraud.

Entities best positioned to collect and share these types of data include payment network operators, core processors, fraud consortia, and regulators. These organizations have the infrastructure, expertise, and reach necessary to gather and disseminate critical fraud data across the payment ecosystem. By leveraging these entities and focusing on these key data sets, stakeholders can significantly enhance their ability to combat payments fraud and protect consumers and businesses.

Payments Fraud Data Collection and Information Sharing (RFI Question #20)

Is there a need for centralized databases or repositories for the sharing of payments fraud data across entities? What legal, privacy, or practical risks and challenges could such a centralized database or repository pose? Which entities are best positioned to develop and participate in a centralized database or repository?

The establishment of centralized databases or repositories for the sharing of payments fraud data across entities could provide significant benefits. Unified access to such a repository would enable faster cross-institution alerts and improve trend analysis, allowing stakeholders to identify and respond to emerging fraud patterns more effectively. By consolidating data, institutions could gain a more comprehensive understanding of fraud activities, enhancing their ability to protect consumers and businesses.

However, there are notable risks and challenges associated with centralized databases. These include the potential for data breaches, which could expose sensitive information, as well as the complexity of governance required to manage such a repository. Ensuring equitable participation among entities of varying sizes and resources is another challenge that must be addressed to ensure the repository's effectiveness and inclusivity.

To mitigate these risks, robust encryption and role-based access controls should be implemented to protect sensitive data. Multi-stakeholder governance structures would ensure that all participants have a voice in the management and

operation of the repository. Additionally, legal safe harbors should be established to encourage participation by protecting entities from liability when sharing data in good faith.

Neutral operators, such as the FRB or an industry-governed utility, are best positioned to develop and manage such a centralized database, with appropriate oversight from regulators. These entities can provide the impartiality and expertise needed to ensure the repository operates effectively and securely. By addressing these considerations, a centralized database for payments fraud data could become a powerful tool in combating fraud and enhancing the resilience of the payments ecosystem.

Payments Fraud Data Collection and Information Sharing (RFI Question #21)

How can the Reserve Banks enhance their existing risk management tools and services, operations, rules, or procedures to better meet the needs of participating financial institutions in addressing payments fraud? For example, should the Reserve Banks consider requiring fraud reporting for payment rails (as they already do for the FedNow® Service) or adopting any particular payments fraud standards?

To enhance their existing risk management tools and services, operations, rules, and procedures, the Reserve Banks should consider extending fraud reporting requirements to all Reserve Bank payments rails. Expanding these requirements beyond the FedNow Service would provide a more comprehensive view of fraud activities across all payment systems, enabling participating financial institutions to better detect and mitigate fraud. This extension would ensure that fraud reporting is consistent and standardized across all payment rails, improving the overall effectiveness of fraud prevention efforts.

Integrating fraud trend alerts into operator portals and APIs is another critical step. By providing real-time alerts on emerging fraud patterns, the Reserve Banks can equip financial institutions with timely and actionable insights. This integration would allow institutions to respond more quickly to evolving threats, minimizing potential losses and enhance the resilience of the payments ecosystem.

Regularly reviewing and updating participant rules to embed evolving fraud standards is also essential. As fraud tactics continue to evolve, participant rules must be adapted to reflect the latest best practices and technological advancements. This ongoing review process would ensure that financial institutions are equipped with the most effective tools and guidelines to combat fraud.

Additionally, the Reserve Banks should provide post-transaction monitoring support with flagging and interdiction tools. These tools would enable financial institutions to identify and address suspicious activities after transactions have been initiated, further strengthening their fraud prevention capabilities. By implementing these measures, the Reserve Banks can better meet the needs of participating financial institutions and enhance the overall security and integrity of the payment system.

Payments Fraud Data Collection and Information Sharing (RFI Question #22)

Are there risk management tools or services that the Reserve Banks should consider offering or expanding, such as (a) developing a payments fraud contact directory for financial institutions, (b) offering tools that can provide notification of atypical payment activity, or (c) introducing confirmation of payee services to help mitigate fraudulent payment origination?

The FRB should consider offering or expanding several risk management tools and services to better support financial institutions in addressing payments fraud. One valuable initiative would be the development of a payments fraud contact directory for financial institutions. This directory would facilitate rapid institution-to-institution escalation, enabling financial institutions to quickly coordinate and respond to fraud incidents. Such a resource would enhance collaboration and improve the speed and efficiency of fraud mitigation efforts.

Another important tool would be the provision of real-time anomaly detection alerts for atypical payment activity. These alerts, offered on a voluntary or opt-in basis, would allow financial institutions to identify and address suspicious transactions as they occur. By providing timely notifications, the Reserve Banks could help institutions minimize losses and prevent fraudulent activities from escalating.

The introduction of confirmation of payee or account name matching services is another critical step to reduce misdirection fraud. These services would verify that the account name matches the intended recipient, adding an additional layer of security to payment processes. This measure would help prevent payments from being sent to fraudulent or incorrect accounts, protecting both consumers and businesses.

Finally, the FRB could offer model validation support for community banks implementing anti-fraud analytics. Smaller institutions often face resource constraints when adopting advanced fraud detection technologies. By providing validation support, the Reserve Banks could help community banks ensure the effectiveness of their anti-fraud models, enabling them to better protect their customers and the broader financial ecosystem. By implementing these measures, the FRB can play a

pivotal role in enhancing the resilience of the payment system and mitigating the risks associated with payments fraud.

*****

We thank you for your consideration of these comments and would be happy to discuss these issues further.

Sincerely,

Bill Hulse
Senior Vice President
Cener for Capital Markets Competitiveness
U.S. Chamber of Commerce