TCH Public

September 18, 2025

Via Electronic Delivery

Office of the Comptroller of the Currency
Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation

Re: Request for Information on Potential Actions to Address Payments Fraud; Docket ID OCC–2025–0009; Docket No. OP–1866; RIN 3064–ZA49

On behalf of our member financial institutions, The Clearing House Association L.L.C.[1] appreciates the opportunity to respond to the Request for Information on Potential Actions to Address Payments Fraud (the "Payments Fraud RFI")[2] issued by the Office of the Comptroller of the Currency (the "OCC"), the Board of Governors of the Federal Reserve System (the "Board"), and the Federal Deposit Insurance Corporation (the "FDIC," and, together with the OCC and the Board, the "Federal Banking Agencies").

I. Introduction

As the ways consumers and businesses communicate about and make payments have evolved, so have the methods of perpetrating payments fraud. It is important to recognize that payments fraud encompasses a range of schemes and mechanisms. In today's environment, payments fraud is no longer limited to manipulation or compromise of payment instruments, instructions, or financial account information resulting in unauthorized payments. While traditional methods of payment instrument and account credential compromise continue, today, payments fraud also includes various schemes targeting consumers and businesses through multiple communication methods outside of banking channels and before consumers or businesses initiate a payment.

The Payments Fraud RFI defines "payments fraud" as "the use of illegal means, including intentional deception, misrepresentation, or manipulation, to make or receive payments for personal gain" and notes that it "includes scams, a subset of fraud."[3] However, there are important distinctions between unauthorized payments and authorized scam payments that impact industry's ability to detect, prevent, and mitigate payments fraud.[4] An "unauthorized payment" occurs when an unauthorized person initiates a payment from the customer's account (such as through account takeover, by using a stolen debit card,

[1] The Clearing House Association L.L.C., the country's oldest banking trade association, is a nonpartisan organization that provides informed advocacy and thought leadership on critical payments-related issues. Its sister company, The Clearing House Payments Company L.L.C., owns and operates core payments system infrastructure in the United States, clearing and settling more than $2 trillion every business day.

[2] Request for Information on Potential Actions to Address Payments Fraud, 90 Fed. Reg. 26293 (June 20, 2025).

[3] *Id*. at 26294.

[4] The Payments Fraud RFI does not include definitions for unauthorized payments or authorized scam payments. We have defined those terms for purposes of our comments because we believe there are important distinctions between the two.

or by initiating a payment after authority to do so has been revoked). An "authorized scam payment" occurs when the customer initiates a payment from their account in response to a scam (such as a text message requesting payment of nonexistent unpaid tolls, an online merchant advertising fake goods, or a social media post promising a guaranteed return on a spurious investment). Unauthorized payments have historically been the primary method of payments fraud, but authorized scam payments are rapidly becoming more common as they do not require fraudsters to gain access to individual account numbers or access devices. Rather, fraudsters can target large numbers of consumers and businesses through a single scam and collect substantial amounts from authorized scam payments.

The financial services industry has been leading efforts to mitigate the impacts of payments fraud. Financial institutions educate consumers and businesses about common fraud schemes, provide warnings about sending payments to unknown recipients, and work with customers and other financial institutions to recover funds lost to fraud, including scams. Financial institutions also employ various tools and strategies to detect and prevent payments fraud, including transaction monitoring, security procedures, and positive-pay services.

In addition to the role of financial institutions in combatting payments fraud, payment network operators have implemented and expanded network rules to address the changing payments fraud environment. For example, some payment network rules shift liability from financial institution participants that would otherwise be liable for fraud losses under federal or state laws to those participants better positioned to prevent the fraud. Some network rules also impose fraud monitoring obligations on participants and require reporting of fraudulent transactions.

Industry organizations, working groups, and other stakeholders have come together to identify ways to detect, prevent, and mitigate payments fraud. For example, the Aspen Institute's National Task Force on Fraud and Scam Prevention is working "to develop the first coordinated U.S. national strategy aimed at stopping financial fraud at its root."[5] The task force brings together various stakeholders, including financial institutions, payment network operators, government, merchants, social media companies, telecommunications carriers, and consumer groups. And the Financial Services Information Sharing and Analysis Center ("FS-ISAC") provides an information-sharing network for financial institutions to discuss cybersecurity and report cybersecurity incidents.[6]

Despite efforts such as these, payments fraud continues to be a significant issue. As discussed in the Payments Fraud RFI, the Federal Trade Commission (the "FTC") has reported that "noncard payments fraud increased 271 percent between 2020 and 2024" and the Financial Crimes Enforcement Network ("FinCEN") has reported "that the number of Suspicious Activity Reports [("SARs")] filed related to check, ACH, and wire fraud have increased 489 percent between 2014 and 2024."[7] The Payments Fraud RFI also notes that "[n]umerous sources report increasing levels of check fraud in recent years, despite overall decreases in check usage."[8]

---

[5] Aspen Institute National Task Force on Fraud and Scam Prevention, https://fraudtaskforce.aspeninstitute.org/about.

[6] FS-ISAC, https://www.fsisac.com/about-us.

[7] Request for Information on Potential Actions to Address Payments Fraud, 90 Fed. Reg. 26293, 26294–26295 (June 20, 2025).

[8] *Id*. at 26295.

As further discussed below, the financial services industry cannot stop payments fraud on its own. A coordinated, national strategy that involves government, law enforcement, and private stakeholders from all relevant industries is needed. Beyond the financial services industry, companies from other industries should also be included in fraud prevention efforts, such as social networking platforms (including social media and online dating companies), online retail marketplaces (such as ecommerce retailers selling goods and services to consumers and businesses), peer-to-peer marketplaces (such as websites allowing consumers to advertise or sell goods and services to other consumers), telecommunications carriers (such as telephone and email service providers), and large retailers. The Federal Banking Agencies can support antifraud efforts by engaging other federal and state agencies, facilitating collaboration across these various industries, and promoting engagement by all stakeholders that can contribute to fraud prevention solutions and fraud loss mitigation.

II. External Collaboration

No single agency, entity, or industry can address payments fraud on its own. Collaboration across agencies, entities, and industries is critical to detecting, preventing, and mitigating payments fraud. To date, much of the effort to combat payments fraud has been focused on the financial services industry. This approach, which generally targets the execution step in payments fraud (i.e., when money is moved), fails to account for the changing nature of how certain modern payments fraud is often set in motion prior to a customer's payment instruction and does not engage other critical stakeholders that could identify and prevent fraud, and particularly scams, at inception.

While the financial services industry has an important role to play in detecting, preventing, and mitigating payments fraud, it is critical to broaden the pool of relevant stakeholders that need to be involved in establishing a collaborative approach to combatting payments fraud.

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

Other stakeholders do not demonstrate the same level of commitment as financial institutions to detecting, preventing, and mitigating payments fraud. Financial institutions are liable to consumers when unauthorized payments occur and are often the primary point of contact for their customers in connection with payments fraud. Financial institutions frequently suffer adverse reputational consequences when their customers are victims of fraud and scams, even when a scam bears no relationship to the financial services industry (beyond the payment the customer instructed in response to the scam). These legal and reputational risks incentivize financial institutions to establish robust fraud prevention programs. Other stakeholders, such as social networking platforms, online retail and peer-to-peer marketplaces, telecommunications carriers, and large retailers, are not subject to the same legal and reputational consequences when their services are used to perpetrate fraud or scams. Without regulatory oversight and reform, these stakeholders are unlikely to independently establish fraud prevention programs or collaborate with the financial services industry on a coordinated payments fraud strategy. Incentivizing these other stakeholders to establish fraud prevention programs and collaborate across industries, such as through stringent regulatory oversight, would help ensure all relevant stakeholders are doing their part to detect, prevent, and mitigate payments fraud.

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?

Stakeholders want to share and receive more information about payments fraud but lack a comprehensive forum to do so. While forums to share information exist, such as through FS-ISAC, the Internet Crime Complaint Center ("IC3"), the National Cyber-Forensics and Training Alliance, and payment network operators, not all stakeholders have access to the same forums or information. Establishing a centralized forum through which all stakeholders can share and receive information would substantially improve collaboration and information sharing.

Confidentiality, data privacy, and litigation concerns are significant obstacles for financial institutions when collaborating to combat payments fraud. Institutions often have concerns about sharing customer data due to federal and state privacy laws and would benefit from broader, more explicit exceptions to these laws for payments fraud prevention and mitigation efforts. Additionally, financial institutions have raised the possibility that self-reported payments fraud data could be used against them in supervisory examinations, enforcement actions, or private litigation; institutions would benefit from assurances that information shared through a centralized forum would be secure, remain confidential, and not be used adversely against them.

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?

Law Enforcement

Federal and state law enforcement agencies are critical to combatting payments fraud. Financial institutions rely on collaboration with law enforcement agencies to help identify, stop, and prosecute fraudsters. There are a few ways that this collaboration could be improved.

First, timely exchange of information between financial institutions and law enforcement is often critical to identifying fraudsters and preventing additional harm. Financial institutions often find that lack of standardization in the information requested by law enforcement and the law enforcement contacts with which to exchange information slow the process and impede effective collaboration. Institutions would benefit from standardized information requests and communication protocols across federal and state law enforcement agencies to ensure better collaboration and more timely responses.

Second, collaboration between financial institutions and law enforcement agencies[9] would be significantly improved if the agencies established specialized fraud liaison roles. These liaisons could ensure continuous communication, clarify jurisdictional responsibilities, and expedite information exchange for swift, coordinated action. To support this collaboration, the law enforcement liaisons could work with industry to conduct regular cross-sector simulation drills to build trust, improve communication, and identify protocol gaps.

[9] Such agencies should include the Federal Bureau of Investigation, the U.S. Secret Service, FinCEN, the Department of Homeland Security, the U.S. Postal Inspection Service, the U.S. Securities and Exchange Commission, and state and local cybercrime units.

Finally, financial institutions would benefit from receiving more feedback from law enforcement about the SARs they file. This is true for all types of suspicious activity that financial institutions report. With respect to fraud in particular, financial institutions file a significant number of fraud-related SARs—and invest substantial resources to do so—yet the value of those SARs to law enforcement is often unknown to the filing institutions. Having insight into which fraud-related filings are most valuable and why would help financial institutions apply their resources in a way that most effectively enables law enforcement to identify, stop, and prosecute fraudsters.

Telecommunications Carriers, Social Networking Platforms, Online Marketplaces, and Other Stakeholders

Many fraud schemes and scams start outside the financial services industry. Fraudsters are frequently using the telephone, email, social networking platforms, and online retail and peer-to-peer marketplaces to target consumers and businesses. Fraudsters are also leveraging developments in generative artificial intelligence ("gen AI") to perpetrate fraud and scams since gen AI can be used to create realistic images, videos, and voices. For example, fraudsters can create fake videos to facilitate a romance or imposter scam or to replicate the voice of a trusted person to entice a victim to make an authorized scam payment. The companies that provide these services or operate these websites and platforms have access to critical information about fraud schemes and are vital to identifying and stopping the fraudsters. For example, a social media platform sharing information about a person suspected of using its dating website to facilitate an investment scam could help a financial institution identify a customer receiving authorized scam payments related to the scam.

These stakeholders can also help support fraud mitigation efforts by detecting and removing fraudulent users and stopping fraudulent activities. For example, telecommunications carriers should prevent fraudsters from spoofing telephone numbers to appear as if a phone call is coming from a legitimate business, internet search engines should block fraudulent websites from appearing as legitimate results in web searches, and online marketplaces should inhibit fraudulent merchants from selling fake, counterfeit, or nonexistent goods on their marketplaces. Imposing stronger fraud prevention incentives and obligations on such companies, such as know-your-customer ("KYC") obligations, would help ensure such companies are taking responsibility for their role in preventing fraud.

Consumer Reporting Agencies

Consumer reporting agencies ("CRAs") house substantial amounts of information about customers that could be used to help detect, prevent, and mitigate payments fraud. Financial institutions rely on CRAs to obtain information about customers to comply with KYC obligations. To help institutions prevent fraudsters from gaining access to the financial system, CRAs must provide comprehensive fraud and identity information. CRAs must also collaborate with other stakeholders, such as telecommunications carriers, social networking platforms, and online retail and peer-to-peer marketplaces, to facilitate the efforts needed of those stakeholders to ensure fraudsters do not gain access to their services and to collect information from those stakeholders about potentially fraudulent customers. For example, information from a CRA could help a telecommunications carrier determine whether a customer applied for an account with a synthetic identity.

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

Federal Banking Agencies

The Federal Banking Agencies should work together to set consistent guidance, establish standard payments fraud terminology, and gather relevant stakeholders across industries to promote collaboration and consistency in reporting and information sharing. One way the Federal Banking Agencies can pursue these goals would be to support recognizing payments fraud as a national security concern—as other countries like the United Kingdom and Australia have done—and the need for a person or agency at the federal level to be responsible for leading antifraud efforts.

Law Enforcement

Fraud schemes often originate online or by telephone and rarely involve a single, local jurisdiction. Financial institutions have experienced challenges in collaborating with law enforcement because, on the one hand, local law enforcement often lacks expertise or reach, and, on the other hand, federal law enforcement frequently does not prioritize fraud cases because the dollar amounts involved are too low. Improved collaboration between federal and state law enforcement agencies, along with a coordinated federal strategy that includes dedicated resources, is needed to target modern payments fraud schemes. Law enforcement would also benefit from greater education about payments systems and payment methods in general and about how such systems and methods can be used to facilitate fraud in particular.

Other Federal Agencies

The FTC and the Federal Communications Commission (the "FCC") should take a more active role in ensuring that the stakeholders they regulate are held accountable for their roles in detecting, preventing, and mitigating payments fraud. All stakeholders should have incentives to implement robust fraud prevention programs and to share information related to payments fraud. For example, the FTC and FCC could more proactively oversee social networking platforms, online retail and peer-to-peer marketplaces, telecommunications carriers, and retailers that fail to implement sufficient fraud prevention programs or to remove users engaged in fraud from their sites or services. The FTC and FCC could also implement KYC obligations on the entities they regulate in connection with activities known to be frequently used in fraud schemes (such as bulk texting and peer-to-peer marketplace sales). These efforts would support a holistic approach to combatting payments fraud that encourages involvement from all stakeholders.

The Consumer Financial Protection Bureau (the "CFPB") should also take an active role in supporting antifraud efforts beyond traditional depository institutions. The CFPB could help facilitate coordinated payments fraud consumer education campaigns through its website and connections with state consumer protection agencies and consumer rights groups. In its supervisory capacity, the CFPB could also ensure that CRAs and nonbank financial services providers implement fraud prevention programs.

The Federal Banking Agencies, FTC, FCC, and CFPB should closely collaborate to ensure consistent expectations, standards, and obligations apply across all relevant industries.

III. **Consumer, Business, and Industry Education**

To be effective, educational efforts need to address all aspects of payments fraud, including how fraudsters are contacting consumers and businesses, the payment channels most susceptible to fraud, the differences between unauthorized payments and authorized scam payments, and liability when fraud occurs. While financial institutions provide various types of payments fraud education, other stakeholders need to be more involved. A coordinated approach to education across stakeholders would promote a consistent message that everyone has a role to play in stopping payments fraud and that payments fraud is a national concern. Educational information should be carefully balanced to ensure appropriate information is provided to consumers and businesses while still protecting critical information, so fraudsters do not leverage it to circumvent antifraud efforts.

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?

Consumers

Payments fraud education should be short, clear, and focused on a particular topic or issue. Education is more effective when it is interactive, includes specific examples, and comes from a trusted source. Education should be distributed via a variety of channels (such as online, billboards, mail, and television) to reach all consumers. Education should strengthen consumers' ability to identify red flags, offer mitigation strategies, and be easily adapted to match the evolving nature of payments fraud.

Businesses

Payments fraud education should be tailored to the fraud risks businesses encounter and the payment channels they use. Business customers should also be educated on the specific tools their financial institution uses to detect and prevent fraud, such as authentication requirements and security procedures, and the internal controls their businesses should employ to benefit most from those tools.

Education Campaign Providers

Financial institutions and payment providers are well positioned to and frequently do provide customer education, including at the time payments are initiated. This education is typically tailored to the fraud risks associated with the type of customer in question, the type of payment, and the method of payment initiation. Specific examples include warning customers to send funds only to people they know, advising customers of common fraud schemes relevant to the specific payment type being initiated, reminding customers not to share any authentication information (such as one-time passcodes), and disclosing the customer's liability for payments. Other stakeholders are better positioned to support broader payments education campaigns that target consumers and businesses before they consider engaging in any financial transaction. This broader education could be disseminated by the United States Postal Service, television, social media, law enforcement, and schools. Implementing a national strategy for payments fraud education would promote the importance of the information and a consistent message.

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?

General education about differences among payment channels would help consumers and businesses make more informed decisions. For example, making payment to a third party via an electronic person-to-person transfer platform as opposed by check may impact a customer's ability to stop payment, liability in the event of a dispute, and ability to recover funds. Customers often do not understand these differences when making choices about how to pay third parties. Customers would benefit from better education regarding different ways to make payments, the pros and cons of each payment method, and use cases for each payment method.

Consumers would also benefit from more education about the differences between unauthorized payments and authorized scam payments. Historically, consumers have used only payment methods leveraging debit (pull-payment) systems (e.g., checks, debit cards, and ACH debits), where the fraud that occurs is mostly due to unauthorized payments and where consumers are generally afforded protection against losses from unauthorized payments. As consumers increasingly migrate toward payment methods leveraging credit (push-payment) systems (e.g., electronic person-to-person transfer platforms), consumers may not understand that fraud is more likely to be perpetrated through authorized scam payments and that the protections available for unauthorized payments do not apply to authorized scam payments. To ensure consumers are taking a more active role in preventing payments fraud and to promote safe payment practices, consumers would benefit from more education regarding scams and steps they can take to mitigate payments fraud. While financial institutions often provide such education at the time of a payment is initiated, consumers would benefit if other stakeholders provided similar education earlier or in other contexts, such as on social media platforms where such scams are often launched.

Education about the importance of reviewing account statements and reporting errors timely would also help ensure customers are doing their part to mitigate payments fraud. A customer may be more likely to recover funds if their financial institution can promptly connect with the receiving institution and law enforcement. The institution cannot do so, however, unless the customer has informed it that something is amiss.The timeliness of customer reporting can also affect the customer's liability. Customers would benefit from more education about their responsibilities in detecting and reporting unauthorized payments and authorized scam payments. Financial institutions remind customers of these obligations, but other financial services providers (such as digital wallets, payment app providers, prepaid account providers, and investment companies) should also act on their responsibility to educate customers.

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?

Payments fraud education could be more effective through proactive engagement and consistent, repetitive messaging. Often, payments fraud education and resources are made available on a financial institution's or government agency's website and customers may seek out or give attention to such information only after they have experienced fraud or fallen victim to a scam or in connection with a specific transaction. Payments fraud education is more effective when it is provided through channels customers are more likely to interact with and heed on a frequent basis, especially before they experience fraud. As customers interact more frequently with other stakeholders, such as social networking platforms

or online retail and peer-to-peer marketplaces, those stakeholders are better positioned to regularly provide broader education before fraud occurs.

All stakeholders should be involved in providing payments fraud education. Financial institutions can reach their customers through their websites, emails, banners, and popups within online banking experiences. But these efforts are limited to the financial institution's own customers and to those occasions on which those customers interact with the institution's online banking services. Other stakeholders are needed to ensure education reaches all consumers and businesses regardless of where they bank, how they bank, or whether they have a traditional bank account.

Law enforcement and other federal and state agencies should support these educational efforts by collaborating to provide uniform resources to all stakeholders. Given limited and often fragmented information sharing, financial institutions often create their own resources addressing common fraud schemes and prevention efforts, which means these resources vary widely between institutions. Uniform resources that stakeholders could disseminate to customers would be beneficial because they would promote consistent messaging across industries and ensure all consumers and businesses have access to important information about fraud and prevention efforts.

Stakeholders should also consider providing more targeted outreach in connection with other communications. For example, a brokerage firm offering a seminar to newly retired individuals could partner with a telecommunications carrier to include information about detecting and reporting telephone-based or text-messaging scams. A mortgage company offering education to first-time home buyers could partner with a social media company to include information about common online scams targeting homeowners. Federal and state agencies should encourage such collaboration.

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

Payments fraud education should not be limited to online resources. While many consumers and businesses rely on online communications, a diverse approach to communicating about payments fraud is necessary to ensure all consumers and businesses have access to appropriate and effective education and resources.

Consumers and businesses would also benefit from a centralized resource on payments fraud. While individual stakeholders can provide targeted education and information, a centralized resource would ensure that all consumers and businesses have access to timely, comprehensive information. For example, a single website, such as one operated by the CFPB, could be created where consumers and businesses can access payments fraud education, information about common scams and fraud schemes, and tips for preventing payments fraud. Individual stakeholders could promote the website through their own payments fraud education and information communications.

IV. **Regulation and Supervision**

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?

10. The Board, FDIC, and OCC have issued supervisory guidance on numerous topics that relate to payments fraud detection, prevention, and mitigation. 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?

11. How might new or revised supervisory guidance assist small community banks in detecting, preventing, and mitigating payments fraud?

The Federal Banking Agencies should focus their efforts on facilitating better information sharing among stakeholders and encouraging other federal and state agencies and stakeholders to play a more active role in detecting, preventing, and mitigating payments fraud. Cross-industry collaboration with standardized fraud reporting would more effectively address payments fraud. The Federal Banking Agencies should also engage Congress and the Executive Branch to support these efforts and to establish a national strategy for combatting payments fraud.

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.)

    (a) For instance, how frequently are consumers and businesses affected by holds, delays, or account freezes, and how responsive are supervised institutions to inquiries from consumers and businesses regarding these issues?

    (b) Do current disclosure requirements effectively address consumer and business concerns when supervised institutions hold customer funds due to suspected payments fraud? For example, should changes be considered with respect to permissible customer communications under SAR confidentiality rules?

Financial institutions may rely on deposit holds, funds availability delays, and account freezes to mitigate the impacts of fraudulent transactions in the payments ecosystem and to investigate potential fraud schemes. Institutions inform customers of such holds, delays, and freezes and respond to related customer inquiries. Current disclosure requirements effectively address this process. Given the fraud and litigation risks involved in employing these tools, even if a financial institution were permitted to share more information regarding suspected fraud with its customers, the institution would be hesitant to do so since these situations often involve investigations into the institution's own customer.

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?

Some financial institutions have raised concerns about challenges with interbank disputes related to fraudulent check claims. Neither the Uniform Commercial Code (the "UCC"), as adopted by each state,

nor Regulation CC establishes a deadline for a financial institution to respond to an interbank check fraud dispute. Both the UCC and Regulation CC contemplate that check fraud disputes will be resolved through bank-to-bank claims or litigation, which are often not efficient or effective, particularly for smaller-dollar-value claims. Some check clearing network rules have attempted to fill this gap by providing processes for network participants to more efficiently resolve check disputes. Rather than amend Regulation CC, the industry should consider appropriate expansion of or changes to the existing adjustments process established under check clearing network rules, including the ECCHO® rules and Federal Reserve Operating Circular 3, and the establishment of a collective resource to support the efficient administration of the check warranty claims process.[10]

For example, under check clearing network rules, network participants may use the check adjustments process for specified reasons, such as to correct errors or discrepancies. At present, there is no general fraud adjustment reason under this process (e.g., for a UCC transfer or presentment warranty claim that the check was altered or an indorsement was forged). Consequently, paying banks may attempt to recover check fraud losses by using check return processes (which results in an automatic chargeback of the credit provided to the depositary bank), even after expiration of the applicable return deadline. This may result in the depositary bank initiating a late return adjustment claim, which can be rejected by the paying bank even if it did return the check late (i.e., outside of required return timelines). It may be appropriate to revise check clearing network rules to prevent paying banks from denying late return adjustment claims when the return was in fact late, ensuring that the paying bank must use the appropriate breach-of-warranty claim process in connection with such claims. Adding a fraud reason to the adjustments process would incentivize paying banks to utilize the proper process by providing an automated mechanism (namely, the adjustments process) through which paying banks could make warranty claims for altered checks or checks bearing forged indorsements. As with other adjustment reasons, the check clearing network rules could establish deadlines for making and responding to claims and information requirements for making such claims. We note, however, that these issues require careful review and consideration by industry representatives with operational, legal, and compliance expertise in check-related issues.

The Federal Banking Agencies should also promote use of industry check claims databases, such as the ABA Fraud Contact Directory,[11] that allow financial institutions to identify the contacts at their institutions that are responsible for check claims processing and through which financial institutions can provide information for submitting check claims to other institutions, such as where to send claims and applicable documentation requirements. Institutions seeking access to such databases should be required to provide a contact person as a condition of access.

Financial institutions would also benefit from clarity on the treatment of washed checks that include both alterations (such as a change in the payee's name or amount of the check) and a forged drawer's signature. Today's electronic check processing environment has made it more difficult for banks to identify issues because the original paper check typically is not inspected or presented for payment; only an image of the check is handled. Further, with the expansion of remote deposit capture services,

[10] "ECCHO" is a registered trademark and service mark of The Clearing House Payments Company L.L.C.

[11] The American Bankers Association maintains the ABA Fraud Contact Directory, which "helps financial institutions connect with other institutions to resolve warranty breach claims for checks as well as claims for unauthorized and/or fraudulent transfers for wires, ACH, RTP, or FedNow", available at https://www.aba.com/banking-topics/risk-management/fraud/directory.

even depositary banks may never receive the original paper check for deposit. As a result, there are competing arguments regarding whether washed checks should be treated as altered checks, leaving the depositary bank liable for the check, or as checks bearing a forged drawer's signature, leaving the paying bank liable for the check. The Board could resolve this issue by amending Regulation CC to establish a liability scheme for a washed check that includes both alterations and a forged drawer's signature.

14. 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?

    (a) Have technological advancements in check processing reduced the time it takes for depository institutions to learn of nonpayment or fraud such that funds availability requirements for local checks and nonproprietary ATMs should be shortened?

While improvements in check processing may have reduced the time for financial institutions (in their role as a depositary bank) to learn of nonpayment in some cases, checks are still subject to warranty claims that apply well beyond the return deadlines that inform funds availability. Under the UCC, drawers are still afforded time to receive and review statements and to report fraud to the paying bank. As such, there are currently many cases where the depositary bank learns of a fraudulent check after funds have been made available to the depositor.

Further, fraud monitoring and detection processes that depositary banks may employ to help identify potential check fraud go beyond whether the paying bank will return the check unpaid, and depositary banks need time to make determinations about potential fraud before making funds available. Improvements in collaboration and information sharing may further reduce the time it takes for a depositary bank to learn of check fraud.

Regulation CC's funds availability schedules must balance customer access to funds with the need to protect against fraud. Current requirements and hold exceptions for checks give depositary banks limited time to detect fraud before making funds available, especially as real-time fraud detection is limited. Shortening the availability requirements would reduce even further the time depositary banks have to identify suspected payments fraud and recover funds from the depositor in cases where the institution does learn of nonpayment or fraud before the funds are made fully available to the customer.

    (b) What effects would shortening funds availability requirements have on payments fraud, consumers who rely on timely access to funds, and depository institutions?

Shortening funds availability requirements would give fraudsters faster access to funds and give financial institutions less time to investigate fraud. It could also increase cross-channel risk as fraudsters could more easily exploit the clearing and settlement lag for check deposits with the instant and irrevocable clearing and settlement of outgoing wires or RTP® or FedNow® transfers.[12]

[12] "RTP" is a registered service mark of The Clearing House Payments Company L.L.C. "FedNow" is a registered service mark of the Federal Reserve Banks.

Depositary banks employ their own fraud detection tools and need time to review potentially fraudulent check deposits and make determinations whether a hold is appropriate. Shortening the funds availability requirements would impede depositary banks' ability to conduct such reviews and place appropriate holds.

(c) Are there any changes the Board should consider to the expeditious return requirement to better balance providing expeditious notice to the receiving depository institution with ensuring adequate time for the paying depository institution to investigate potentially fraudulent checks?

Both depositary and paying banks implement processes for detecting and investigating fraudulent checks. Improvements in collaboration, information sharing, and the adjustments process would be beneficial. Drawers often have 30 to 60 days to review account statements and report fraudulent checks to the paying bank.[13] Without shortening the timeframe within which a drawer must report fraud to the paying bank to correspond to return timing requirements, which we do not believe to be desirable for customers, paying banks will not be able to return all fraudulent checks within the expeditious-return timeframes. Facilitating better information sharing and communication between institutions would help paying banks more quickly inform depositary banks of fraud and would allow depositary banks to take more timely action in response. Adding a fraud return reason to the adjustments process could also further improve timeliness and responsiveness as it would provide an automated mechanism for a paying bank to notify a depositary bank of a fraudulent check and for the institutions to resolve the dispute.

15. 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. 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?

Financial institutions would benefit from regulatory guidance on the applicability of the reasonable-cause-to-doubt-collectability exception. The current commentary primarily focuses on items being uncollectible for reasons other than fraud, such as stop payment orders, insufficient funds, and stale-dated checks, with limited fraud-related examples in the model form hold notice, such as indorsement issues and apparent alterations.[14] Financial institutions would benefit from clearer guidance on the use of this exception in the context of fraud, including where depositary and paying banks identify fraud risk through the use of modern fraud detection models that incorporate broader fraud risk factors about accounts or customers. For example, fraud models often consider factors unrelated to the specific check deposit, such as how long the account has been opened, whether other checks or deposits have been returned, and account balance history. Institutions would benefit from guidance that fraud models like

[13] Under UCC § 4-406, a customer has a duty to promptly examine their account statement and report whether the payment was unauthorized because of an alteration or because the drawer's signature was not authorized. Furthermore, section 4-406 precludes a customer from asserting a claim more than one year after the statement was made available. In practice, many banks shorten this period in their customer agreements.

[14] *See* 12 C.F.R. Part 229, Appendix C, Model Form C-13.

these may be used to support a determination that the institutions have reasonable cause to doubt collectability of a particular check deposit.

Financial institutions continue to report high rates of fraud in connection with Treasury checks. As Treasury checks are subject to next-day availability, depositary banks have little time to review these checks and make determinations about their validity. Furthermore, as Treasury is not subject to Regulation CC's expeditious-return requirements, a depositary bank may not learn of nonpayment on a Treasury check before it is required to make funds from the deposit available. Depositary banks would benefit from additional time to review Treasury checks before making funds available to customers.[15]

Financial institutions would also benefit from greater legal clarity and added flexibility to hold electronic payments when there is a reasonable suspicion of fraud. The Board and CFPB could amend the interpretation of when an electronic payment is received under the Expedited Funds Availability Act ("EFAA") and Regulation CC to add a third prong under 12 C.F.R. § 229.10(b)(2) such that payment is not received until the bank has (i) received "payment in actually and finally collected funds"; (ii) received "information on the account and amount to be credited"; and (iii) complied with the bank's policies on reasonable fraud screening processes. This third prong would allow banks to use fraud screening tools to detect potentially fraudulent transactions and investigate those transactions before making the funds available.

V. **Payments Fraud Data Collection and Information Sharing**

Data collection and information sharing are critical to detecting, preventing, and mitigating payments fraud. The Federal Banking Agencies should support better access to information and facilitate information sharing across all relevant industries, not just the financial services industry.

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

Stakeholders would benefit from improved infrastructure for data sharing, and stakeholders outside the financial services industry should be incentivized to report data and share information related to payments fraud.

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 bilateral or multilateral payments fraud data collection and information sharing? What changes would address these barriers?

Privacy Laws

Federal and state privacy laws may prevent stakeholders from sharing payments fraud information. For example, privacy laws apply to all customers, including customers engaged in fraud, which may prevent a financial institution from sharing information about its customers. Stakeholders would benefit from clear exceptions and safe harbors to facilitate information sharing in connection with antifraud efforts. For example, privacy laws could be amended to create a safe harbor similar to the

[15] Next-day availability for Treasury checks is established by the Expedited Funds Availability Act, 15 U.S.C. § 4002(a)(2)(A), and statutory amendments may be necessary to extend the funds availability requirements for these checks.

regulations implementing section 314(b) of the USA PATRIOT Act[16] that would allow stakeholders to voluntarily share information about suspected payments fraud while protecting those stakeholders from liability in connection with such sharing. This would allow stakeholders, other than just financial institutions, to more readily share information about scams and other payments fraud with each other and with law enforcement.

Data Breach Risk

Financial institutions have concerns about the implications and litigation risks that might arise in the event an unauthorized third party gains access to information the institutions shared with others. We encourage the Federal Banking Agencies to consider these concerns as they work to alleviate barriers to the collection and sharing of payments fraud data.

Customer Service

In certain cases, a financial institution may receive information suggesting an outgoing payment may be part of a fraud scheme, such as a scam. Despite notifying the customer of such concerns, the customer may insist the institution complete the payment. Financial institutions have raised potential litigation, regulatory enforcement, and customer service concerns that they face when failing to comply with customers' payment instructions in these circumstances.

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 Federal Banking Agencies can support standardization of payments fraud data by establishing terminology and definitions, ensuring terminology aligns with regulatory and industry definitions, and promoting consistent use of such terminology in fraud reporting, including SARs and reporting required under Federal Reserve Bank operating circulars. While financial institutions support the development of tools such as the FraudClassifier℠ and ScamClassifier℠ models, widespread adoption of such tools has been limited in part because the terms used in the models do not clearly align with regulatory definitions, such as "unauthorized electronic fund transfer" as defined by the Electronic Fund Transfer Act, or network rules definitions, such as "Unusual Payment Order" as defined in Operating Circular 8.[17] To be more effective, the models should be more clearly aligned with regulations and network rules and applicable to all functions within an entity, including customer-facing functions, such as error resolution and complaints, and back-office functions, such as payments processing and reporting. While standardized terminology should be encouraged, use of any specific model should remain voluntary.

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?

Financial institutions would benefit from additional data to assist in detecting authorized scam payments and the scams that precede customers' initiation of payments. The more information financial

[16] 31 C.F.R. § 1010.540.

[17] "FraudClassifier" and "ScamClassifier" are service marks of the Federal Reserve Banks.

institutions have access to, the better they will be able to build models for detecting and preventing authorized scam payments. As scams often originate outside the financial services industry, data from other stakeholders is critical to assist financial institutions in their efforts. Better infrastructure for data sharing across industries would support these efforts.

Law enforcement, telecommunications carriers, social networking platforms, and online retail and peer-to-peer marketplaces are best positioned to provide this additional data. For example, a telecommunications carrier should share telephone numbers that it knows have been used in connection with scams so financial institutions can block customers from enrolling in person-to-person funds-transfer services using those numbers as the customers' social aliases or can stop payments sent to recipients using those numbers as their social aliases.

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?

All stakeholders would benefit from a centralized database for payments fraud data sharing. While databases and data-sharing programs exist today, they are often limited in scope, in terms of participants, or the payment methods they cover. Additionally, access to data may be limited due to cost or access restrictions. A centralized database would help ensure all stakeholders have access to available payments fraud information. Stakeholders should be obligated to contribute data to the database as a condition of accessing the database to promote its completeness.

A CRA may be best positioned to develop and maintain a centralized payments fraud database. CRAs have experience collecting data from third parties, establishing rules for data collection and reporting, and maintaining vast amounts of data. CRAs are also subject to privacy and data security laws and supervisory oversight. However, a nonprofit organization or government agency might also be well positioned for this role, depending on the nature of the data that is shared and the analytics that are applied to the data. Whatever solution is developed, the Federal Banking Agencies ought to be mindful of the concerns we outlined above concerning the risk of data breaches.

VI. **Federal Reserve Bank Operator Tools and Services**

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?

Many fraud risk management tools focus on the originating institution (e.g., unauthorized debit return rates) rather than the receiving institution. To help identify and mitigate authorized scam payments, the Federal Reserve Banks should consider providing resources or tools to help financial institutions identify and monitor potential authorized scam payments.[18] The Federal Reserve Banks should

[18] The Clearing House Payments Company L.L.C. is taking its own steps along these lines. For example, while reported fraud on the RTP network is minimal, The Clearing House Payments Company L.L.C. is developing an RTP

also consider improving fraud data sharing and collaboration efforts among network operators and across payment systems to better identify trends and fraud risks. In particular, there may be opportunities for the Federal Reserve Banks and The Clearing House Payments Company L.L.C. to collaborate, and we would welcome dialogue on those issues.

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?

While the Treasury Check Verification System ("TCVS") provides a method by which depositary banks can verify the authenticity of a Treasury check, depositary banks report limitations with this process as not all valid Treasury checks are timely reported in TCVS. Moreover, since Treasury checks may be accepted for deposit before a depositary bank can verify the check via TCVS, a depositary bank that learns of a mismatch must decide whether to place a hold on the funds pending a potential return or reclamation claim, which could take months to resolve. As discussed above, Treasury checks are subject to next-day funds availability under Regulation CC even though Treasury is not subject to the expeditious-return requirements applicable to paying banks. Treasury and financial institutions would greatly benefit from Treasury implementing an automated system to ensure expeditious return of Treasury checks, such as a positive-pay service managed by the Federal Reserve Banks that would automatically validate the check number, dollar amount, and payee name of a Treasury check upon presentment and automatically return (before the depositary bank must make funds available to the depositor) any Treasury check that has already been paid or where the information does not match Treasury records. This automated process would also prevent Treasury from having to process late returns or go through the lengthy reclamation process. As Executive Order 14247, *Modernizing Payments To and From America's Bank Account*, mandates that most government payments be made via electronic payment, the decline in the volume of Treasury checks should ease implementation of an automated returns process.[19]

While many different fraud contact directories exist, financial institutions would benefit from a centralized contact directory. The Federal Reserve Banks should promote the development and use of a centralized directory, such as ABA Fraud Contact Directory, that allows financial institutions to identify the contacts at their institutions that are responsible for various aspects of fraud risk management and interbank fraud claims processing. Institutions seeking access to such directories should be required to provide contact information as a condition of access.

VII. **General Questions**

23. What types of payments fraud have most impacted your organization and its stakeholders? What tactics have criminals employed when perpetrating these types of payments fraud?

24. What measures, including technological solutions or services, have been most effective in identifying, preventing, and mitigating payments fraud at your institution? Are there actions that consumers can take that help institutions? For example, do financial institutions find it

network tool to permit sending participants to request specific data elements about a receiver's account to inform risk-based determinations on whether to send an RTP payment to that account.

[19] *See* Modernizing Payments To and From America's Bank Account, 90 Fed. Reg. 14001 (March 28, 2025).

helpful when consumers alert the institution in advance when making large purchases, transferring large amounts of money, and traveling abroad?

25. To the extent not already addressed here, are there other actions that would support stakeholders in identifying, preventing, and mitigating payments fraud?
26. Are there specific actions that commenters believe could encourage the use of payment methods with strong security features?

As payments fraud, including scams, continues to grow and evolve, a coordinated, cross-industry strategy is essential to fraud detection, prevention, and mitigation. Scams and other types of fraud frequently originate outside the financial services industry, so companies that interact with fraudsters at the stage where the fraud begins play a critical role in antifraud efforts. All stakeholders should have obligations based on their ability to detect and prevent fraud. These obligations should include implementing KYC controls, blocking fraudsters from accessing the platforms and services they use to perpetrate fraud, and sharing information about fraudulent activities with other stakeholders. Consumers and businesses also must understand their responsibilities in protecting themselves against payments fraud and timely reporting incidents to financial institutions and law enforcement. The Federal Banking Agencies should take the lead in bringing stakeholders together to collaborate on approaches to prevent fraud, including scams, that involve all relevant stakeholders.

* * * * *

Thank you for the opportunity to comment on the Payments Fraud RFI. If you have any questions or wish to discuss this letter, please do not hesitate to contact the undersigned.

Respectfully submitted,

/s/ Stephen Krebs

Associate General Counsel

[redacted]