September 18, 2025

Jonathan Gould
Comptroller of the Currency, Office of the Comptroller of the Currency
Docket ID OCC-2025-0009

Benjamin W. McDonough
Deputy Secretary, Board of Governors of the Federal Reserve System
Docket No. OP-1866

Jennifer M. Jones
Deputy Executive Secretary, Federal Deposit Insurance Corporation
RIN 3064-ZA49

Dear Mr. Gould, Mr. McDonough, and Ms. Jones:

We are pleased to offer the following comments to the questions posed regarding fraud that is being perpetrated affecting consumers, businesses, banks, other financial institutions and government entities throughout our country. We are responding to hopefully provide perspectives and more information that paired with other responses could lead to a better methodology and a collaboration in the industry to work well together to combat the intrusion of current banking processes and requirements to perpetrate fraud.

We would offer that there are emerging threats that may not be captured in the responses to the questions below to include the use of Artificial Intelligence criminal tools that are available to assist in how fraud is perpetrated as well as assist in making the universe perpetrating fraud to be expanded. The industry needs to take appropriate actions, planning and education regarding those emerging threats and new tools that can make fraud detection more difficult.

We would like to also refer to the Federal Bureau of Investigation Internet Crime Report 2024 as reference for very good statistics and information ragarding fraud statistics by age groups, types and statistics on reported fraud. We have to assume there were more fraud attempts that were not reported and are not reflected in the FBI Report. The amount of fraudulent activity and the increase in reported activity year over year is staggering. I refer you to the following pages in the report to see the detailed information regarding the fraudulent activity reported:

The full Federal Bureau of Investigation 2024 Internet Crime Report can be found here:

ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

Pages 4, 7, 8, 9, 10, 11, 12, 13, 14, 16, 17, 18, 19, 21, 27, 35, 36, 37 and 39. We know we are referring many pages but with each page reviewed the details and analysis allows a more widened view of the amount of fraud that is attempted and the dollar amounts that are being affected each year.

We offer the following comments to the questions posed in the RFI:

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

    - We need common, clear communication channels.
    - We need broad collaboration in the industry to combat fraud. The perpetrators of fraud are using data they collect across the industry to perpetrate fraud. The industry can better protect itself by stronger collaboration of information to combat fraud attempts generically and in real time.
    - The ability to share information that would not violate current information sharing rules, laws or interpretations of those regulatory and legal requirements.
    - Create methods or standards to provide information in a secure, informative manner that does not violate privacy but protects the integrity of the financial system.
    - Review current rules, laws and regulation to allow collaboration and sharing of information to deter and prevent fraudulent activity.

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?
    - The industry needs to have good communication contacts and channels to be able to communicate regarding fraudulent items, mule accounts and attempts real time. This would require real contacts that are available and not generic email addresses only that are not responded to nor have published verbal contact ability to get in touch with a given bank.
    - Having good communication contacts and ability to work directly with a financial institution, law enforcement and government agencies regarding fraudulent activity investigations and maintaining appropriate protocol regarding customer confidentiality and legal procedures.
    - Effective collaboration of National and State Trade Associations working together to facilitate information regarding fraudulent activity and the ongoing refinement of communication resources and Federal Regulatory and Enforcement Resources information that could be made available securely to the industry.

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?

    - Organizations such as FS-ISAC that have various collaborative groups could assist in providing information to the industry from industry knowledge/reported activity cells conducting fraudulent activity and law enforcement channels. Knowledge and awareness of current fraud trends for institution staff of all sizes is critical. Smaller community banks have limited human resources available and do not have time to

research trends, etc. Seamless access to information on a daily basis would be most helpful by all groups.

- FINCEN, Law Enforcement (FBI and others) and the U.S. Postal Service collaborating with industry would assist in closing loopholes for fraudsters to exploit.

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

- Yes. Our industry is bifurcated regarding the topic of fraud. While various agencies and banks have our roles to complete. If we are going to win the day on the prevention of fraud, we need to have timely data of trends and activity by perpetrators to help bankers, tellers, operational staff and fraud prevention teams to become more and more effective in the detection of potential and actual fraudulent attempts in a more real time manner.
- A standard secure system to report fraudulent activity and having a database of accounts that have been used for fraudulent activity would be helpful. This could be housed at the Federal Reserve Bank similar to other fraud reporting requirement for FedNow.

Consumer, Business, and Industry Education

Consumers, businesses, financial institutions, and other industry stakeholders currently have access to education on a range of financial topics, including payments fraud. However, there may be a need for further education specific to peyments fraud. Effective payments fraud education could, for example, help industry stakeholders identify suspected payments fraud and better inform affected parties about what steps to take following an incident of payments fraud. The effectiveness of any payments fraud education, however, may be undermined by the ever-evolving nature of payments fraud, the highly specific and sensitive nature of these crimes, and the range of potentially inconsistent guidance from multiple sources.

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?

- Real stories of experiences of fraud assists institutions to better prepare, execute and revise processes for better detection, suspicion of activity and can result in quicker action on a given potential issue. Education is key for consumers, businesses, financial institutions, law enforcement and all parties in the eco-system.

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?

- Yes, more information and the education of all parties in the eco-system for payments and banking product utilization will assist in preventing fraud. Suspicion awareness and early detection is a first line of defense for fraud attempts. As an industry, we need to continually educate internally and externally regarding fraud prevention. Having access to a central database or reporting structure would benefit the industry and Americans in the prevention of fraudulent activity.

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?

- Conducting education in a collaborative way allows for more awareness, effective distribution of information. Potential advertisement campaigns via social media by financial services national trade associations may get the attention of consumers and business owners. Education from the Federal Regulators would be helpful for the public to hear from the regulatory agencies that banks will never ask for your credentials or your personal private information.

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

- Concise updated payments fraud schemes and processes will be helpful ongoing. Current online education is generic in nature. Targeted and informed concise education would be helpful in the future regarding current tactics being experienced.

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?

- Mandating or requiring that financial institutions provide access and response to other banks regarding inquiries of potential fraud attempts. To date, community banks have not been able to get in contact with larger institutions regarding a potential fraudulent item. It is either very difficult to obtain contacts or if you get a generic email address and there is no specific response. In past decades, financial institutions worked collaboratively to prevent issues such as being experienced in fraud today. This has not been the case with current fraud activity.

- Federal Regulators working with law enforcement could assist by using information available for those perpetrating the fraud to be held accountable legally and working to recover funds stolen.

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?

- The guidance needs more clarity. Financial institutions are working with service providers to combat existing fraud attempts while working collaboratively to adopt updated systems to provide better potential fraud detection of emerging innovations in the industry. One of those emerging applications is instant payments. The faster money moves, more effective fraud prevention techniques and systems as well as regulatory clarity and industry collaboration will be greatly needed. This can be said of rails that have existed for approaching 50 years also.

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

- The ongoing education of customers both consumer and businesses are an ongoing emphasis and a challenge. An idea is if Regulator Agencies, Bank Trade Associations and Small Business Associations work together to expand education efforts regarding fraud prevention.
- New or Revised Guidance provided with clarity of intention/ expectations of the regulatory guidance of community banks as well as providing expected best practices in fulfilling the guidance would be a benefit to the industry and customer base.

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?

- It is in the best interest of the customer, the bank and the bank of first deposit potentially if a bank puts a hold on a questioned or suspected fraudulent item so that appropriate research can be exhausted. This stops a bad item from continuing in the payments system protecting the industry, banks and customers involved.

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?

- Standardized language would be helpful for customers and banks to know the way suspected potential fraudulent items will be handled.

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? Although the Board is not proposing any changes to Regulation CC at this time, the Board seeks comment on the following questions:

- We encounter difficulty locating a contact, getting in contact with a live person and obtaining a timely response from the larger banks regarding an item suspected of potential fraud. Many of the larger banks have a generic email address if a contact is located and no response is received.
- In previous days of banking, a bank representative could contact another institution to verify funds however many banks will not verify funds anymore or deny the legitimacy of a check. This is why we have responded earlier that industry collaboration needs to be emphasized in the industry and by the regulators.

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?

- Suspicious items whether checks, debit card items or ATM transactions require time to review and determine if fraud is being perpetrated. It would not be our recommendation to shorten funds availability at this time due to the quickness of processing and amount of research time to determine item validity.

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

- The shortening of funds availability reduces the ability of financial institutions to research a potential fraudulent item.

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?

- The industry needs clarity for reasonable cause to doubt the collectability of a check. I am sure the reasonable cause exemption is being used in different ways by different financial institutions. Some items take longer to research. Examples and guidance clarity would be helpful. Banks need time to appropriately research suspicious items while maintaining a focus on timely posting of items.
- Reg CC does not define criteria related to endorsements on items which can cause issues if that is not known and a bank does not accept an endorsement resulting in a potential protracted time before an item is returned.

Payments Fraud Data Collection and Information Sharing

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

- Fraud data of suspected items could be included in SAR filings once confirmed that does not violate any other rule, regulation or provision of guidance. This could lead to an established data collection system for fraudulent or suspected fraudulent items to be in a data base that can be referred to in real time to see if other items are filed with the same information.
- If the collected data could be downloaded into each bank's database for use when items are deposited this could allow for more timely recognition of a suspected item after the database became more populated over time.

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?

- Existing privacy laws and regulations prohibit the sharing and release of consumer information. Therefore, banks are conflicted in sharing information while attempting to work with another institution to research and determine if an item is fraudulent.

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 FraudClassifierSM and ScamClassifierSM models?

- Establishing standards for fraud data reporting that is approved by regulation so that banks can work together without concern of violation of any privacy rules/laws. The standardization would allow more consistent data access and resource search tool creation and availability.

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?

- A database of compromised accounts, known fraudsters and their mode of operation.
- Utilization of a created database must be maintained by a restricted pool of payment processing entities within the payments systems to ensure the quality of data is maintained.

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?

- A centralized database is a needed tool for the industry and would be greatly beneficial. The Federal Reserve Bank, The Clearinghouse as well as core processor providers and third-party fraud detection systems have payment information flow through each of their systems. The database could be housed at the Federal Reserve Bank with input provided by other stakeholders in the industry to achieve a fraud database.

Reserve Banks' 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?

- Yes. Require fraud reporting similar to call report filing but just to the Federal Reserve Bank to assist in the creation of a fraud database on all payment rails. There would need to be standards for consistency and having good data to utilize.

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?

- Yes, to each of item's a, b and c. A contact directory would be helpful for use by financial institutions to be able to efficiently research items or discuss fraud with another involved institution.

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?

- The amount of time, money and resources that have been expended on check fraud and debit card fraud has been impactful. ACH fraud detection and research as well as ATM fraud has also been experienced at an increased rate.

We thank you for the opportunity to offer comments regarding this important topic. Thank you for your efforts in gathering information from the industry.

Sincerely,

David Long
Executive Vice President
Correspondent Banking/Capital Markets
Bryant Bank
Tuscaloosa, Alabama