

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:

The Independent Community Bankers of America (ICBA)¹ appreciates the opportunity respond to the Office of the Comptroller of the Currency (OCC)'s, Board of Governors of the Federal Reserve System (Board)'s, and Federal Deposit Insurance Corporation (FDIC)'s request for information (RFI) on payments fraud.

ICBA applauds the agencies for issuing this RFI and seeking input on ways that the OCC, the Federal Reserve System (FRS), and the FDIC could take actions to help consumers, businesses, and financial institutions mitigate payments fraud. Community banks continue to be challenged by a rise in fraud and scams across payment types, so agency action is much needed.

The Request for Information

The RFI requests comment on five potential areas for improvement and collaboration that could help mitigate payments fraud:

- **External collaboration.** The agencies, and particularly the FRS, have a long history of collaborating with stakeholders to support the safety and efficiency of the U.S. payment system. The RFI asks questions about the need for stakeholder collaboration, the types of stakeholders that should collaborate, the types of collaboration that could be effective, and any obstacles.
- **Consumer, business, and industry education.** The agencies acknowledge the significant amount of payments fraud education available to consumers, business, financial institutions, and other stakeholders. The RFI asks questions about the types of education that are most

¹ The Independent Community Bankers of America® has one mission: to create and promote an environment where community banks flourish. We power the potential of the nation's community banks through effective advocacy, education, and innovation. As local and trusted sources of credit, America's community banks leverage their relationship-based business model and innovative offerings to channel deposits into the neighborhoods they serve, creating jobs, fostering economic prosperity, and fueling their customers' financial goals and dreams.

effective, where additional education would be valuable, and how best to target future efforts.

- **Regulation and supervision.** Authority over the U.S. payment system is shared across federal and state agencies. Nevertheless, the OCC, Board, and FDIC do exercise significant authority in the form of supervising financial institutions and promulgating regulations. The RFI asks questions about the need for changes to regulations and supervisory guidance, the effects of holds placed on funds, resolving disputes about fraudulent checks, and Regulation CC.
- **Payments fraud data collection and information sharing.** There is no single, standard mechanism or source for collecting or reporting fraud data. Barriers to collecting data, including operational, legal, and regulatory constraints, make it difficult to provide actionable, centralized fraud data. The RFI asks questions about ways to improve fraud data collection and sharing, barriers, types of data that would be useful, and the need to develop new repositories.
- **Reserve Banks' operator tools and services.** The FRS's 12 Reserve Banks offer a variety of tools and services for fraud prevention, detection, mitigation that sit alongside their check processing, ACH, instant payments, and wire services. The RFI asks questions about additional steps the Reserve Banks could take to address payments fraud.

The RFI also asks a number of general questions about commenters' experiences with fraud and other suggestions for identifying, preventing, and mitigating payments fraud.

ICBA Comments

The payments fraud landscape is evolving rapidly. As payments become faster, community banks are faced with the fundamental tension between speed and security. Similarly, complex cross-border arrangements and non-traditional assets present unique challenges. Fraudsters increasingly make use of advanced technologies and trade information on the dark web.

As a result, fraud and scams are affecting community banks' bottom lines as well as their relationships with customers. But, most importantly, fraud and scams are affecting Main Street. National polling conducted by ICBA and Morning Consult found that one in five consumers have been, or know someone who has been, a victim of check fraud. And four out of five consumers support policymaker action to address check fraud.²

Community banks have a unique advantage that other institutions simply cannot replicate: community banks' deep ties with their local communities help them to fight fraud on the front lines. ICBA has been working hard to help community banks leverage that advantage to prevent, detect, and mitigate fraud and scams and in all forms:

² <https://www.icba.org/newsroom/news-and-articles/2025/07/01/new-icba-polling-shows-public-support-for-policy-efforts-targeting-check-fraud>

- **Fraud Task Force.** ICBA spearheads a fraud task force that brings together community banks and state associations from across the country to share information, build relationships with regulators, and collaboratively develop resources for their peers. Notably, ICBA and the task force have jointly released a series of resources that address check fraud, including a comprehensive guide to liability, a survey of detection mechanisms, and instructions for how to escalate interbank disputes to regulators.³
- **Targeted partnerships.** ICBA also partnered with the US Postal Inspection Service to produce an in-branch handout for community bankers to share with customers and start a conversation about fraud and scams prevention.⁴ Hundreds of thousands of copies have been distributed to hundreds of banks across the country. ICBA continues to pursue targeted partnerships to produce tools and resources to help community banks combat fraud and scams.
- **Education and innovation.** ICBA also continues to deliver a broad range of educational content to help banks develop and implement their strategies to combat fraud and scams, including comprehensive coursework and topical webinars. ICBA's ThinkTECH Accelerator program provides opportunities for early-stage fintechs, including those targeting fraud and scams, to learn from and work with community banks.
- **Advocacy and support.** Finally, ICBA has been steadfast in its advocacy to support community banks' ability to fight fraud and scams on the front lines. ICBA has developed close relationships with the full spectrum of policymakers, and it continues to serve as a valuable source of information about what community banks are seeing in their communities—and what they need to help their customers.

ICBA's suggestions and comments on the five potential areas for improvement and collaboration are as follows:

External Collaboration

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

- **Create a neutral, trusted forum.** Currently, there are numerous industry efforts to address payments fraud broadly and specific types of fraud more narrowly. These efforts can have conflicting goals, draw different sets of stakeholders, and have limited external coordination and communication mechanisms. A single, inclusive, action-oriented forum to centralize industry efforts would be hugely beneficial. However, national efforts must recognize the resource constraints individual community banks face when deciding whether to participate.

³ <https://www.icba.org/our-positions-a-z/current-policies/fraud-and-scams/>

⁴ <https://www.icba.org/newsroom/news-and-articles/2025/02/20/icba-and-u.s.-postal-inspection-service-partner-to-help-community-banks-combat-check-fraud>



- **Support local and regional collaboration.** Local and regional collaboration across community banks, federal and state regulators, law enforcement, community organizations, and other stakeholders can be an effective way to build connections and share information at the community level. Support for these efforts from the joint regulators could add to their visibility and efficacy.
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?*
- **Developing standards for interbank communication and coordination in cases of suspected or confirmed fraud.** Financial institutions are often unsure about what information they are permitted to share and are concerned that open communication could affect their liability. Standards to create structure and certainty around interbank communication and coordination related to fraud would enhance the likelihood and efficacy of information sharing.
 - **Convening federal agencies beyond the joint regulators.** Many federal agencies, including those that address telecommunications, the economy, and law enforcement, could have a valuable role to play in addressing payments fraud. A broad, inclusive federal effort is essential for effectively tackling payments fraud.
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 that serve populations that are disproportionately affected by fraud.** For instance, organizations that serve senior citizens or those that live in rural communities could be valuable collaborators.
 - **Law enforcement organizations.** Organizations that represent the law enforcement community have valuable experience in detecting, preventing, and mitigating payments fraud, and could be valuable collaborators.
 - **Telecommunications and social media companies.** Organizations that represent the telecommunications industry, telecom companies, and social media companies are essential partners in combatting fraud and scams.
4. *Could increased collaboration among Federal and State agencies help detect, prevent, and mitigate payments fraud? If so, how?*
- **Enhanced coordination across agencies could help.** As the RFI notes, the scope of parties involved in payments fraud law, regulation, and supervision is vast. While federal agencies enforce federal regulations, state agencies enforce an array of differing state regulations and laws. Efforts to increase communication and collaboration across
-

different agencies is incredibly important.

- **Harmonized policy could help.** Given the array of laws, regulations, and other policies enforced across the federal and state levels, including the Uniform Commercial Code, there is significant opportunity for conflicts to arise. Conflicting policy leads to uncertainty, increased compliance costs, and uneven enforcement. Collaboration across different agencies could lead to greater harmonization.

Consumer, Business, and Industry Education

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?*

- **Consumer- and business-facing education is effective.** Consumers and businesses should understand the role they play in preventing, detecting, and mitigating fraud. They should also understand their responsibilities. Community banks thrive, in part, because of their close customer relationships, so face-to-face engagement is one of the most effective tools to reach community bank customers. In-branch material and messaging is especially valuable for community banks.
- **Industry-facing education is effective.** Banks should understand their compliance obligations and potential for liability. They should also understand the options they have available through FRS and other third-party payment service providers.

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 for small businesses would be helpful.** Small business customers sometimes face disproportionate fraud risks, especially those businesses that rely on checks. These businesses can be very cash flow-sensitive and could benefit from additional education on fraud risks and mitigation opportunities.

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?*

- **Tailored materials could make education more effective.** Community banks serve elderly customers, as well as consumers and small businesses in rural and agricultural areas, so educational materials tailored to these groups would be valuable.

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

- **Some community bank customers cannot readily access online resources.** Some



community banks are in areas that do not have widespread, reliable Internet access, so web-based resources are not always accessible to customers.

- **In-person and printed materials should be created.** Alternatives to online resources, like in-person and paper-based materials, could help to reach these individuals and businesses. The joint regulators could provide presentations or templates to help community banks disseminate this material.

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?*

- **Tailor regulations appropriately.** Broadly speaking, payments fraud regulations and examiner expectations need to be appropriately tailored to community banks with tiered compliance requirements and deadlines. One-size-fits-all regulations create disproportionate burdens on community banks and fail to focus on their unique fraud patterns.
- **Create new safe harbors.** Regulatory safe harbors should be developed that protect community banks that implement appropriate fraud prevention measures from liability when customers fall victim to scams. This would incentivize community banks to continue to invest in and implement effective fraud prevention, detection, and mitigation mechanisms.

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?*

- **Consolidate supervisory guidance.** As the RFI notes (and cites), the agencies have released guidance across many topics and in a variety of forms. Community banks would benefit either from a single, consolidated supervisory framework or—at minimum—a community bank-specific resource that helps community banks coordinate and comply with the range of guidance that has been issued.
- **Provide guidance on emerging fraud and scams.** In many cases, supervisory guidance is retrospective, addressing fraud and scams that have previously occurred. Community banks would benefit from real-time guidance on how to prevent, detect, and mitigate emerging fraud and scams.
- **Avoid imposing new burdens on community banks.** New or revised supervisory guidance that is particularly burdensome could impact community banks' abilities to effectively prevent, detect, or mitigate fraud by forcing resources to be redirected to



compliance activities.

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

- **Explain how requirements should be applied by community banks.** Supervisory guidance should provide concrete examples for community banks on how to effectively apply supervisory guidance. Because community banks have specific needs and constraints, one-size-fits-all supervisory guidance can be unhelpful to community banks.
- **Establish clear examiner expectations.** Supervisory guidance should clearly explain what examiners will look for related to fraud. Fraud patterns experienced by community banks can be different than other institutions, and suitable fraud programs should be responsive to those threats. A common understanding across examiners and community banks about examination expectations would help community banks build and implement appropriate fraud programs.

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.)*

- **Holds help community banks address payments fraud.** Delaying funds availability is an important tool banks use to detect and mitigate check fraud. Holding checks gives banks an opportunity to review the checks for signs of fraud and investigate any suspicions. If fraud is detected, banks can return checks before customers are affected and prevent the checks from entering the ecosystem.

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?*

- **Community banks have difficulty resolving interbank disputes regarding fraudulent checks.** Community banks report that large financial institutions often reject fraud claims even when they provide significant documentation. In addition, contacts are difficult to find (despite the existence of third-party directories), and communication timeframes are often long. As a result, community banks are often forced to absorb losses when they have legitimate claims.
- **Remote deposit capture is often used to facilitate check fraud.** Remotely deposited checks make it difficult to determine whether a check has been altered. In many cases,



the physical item is not available for banks to examine. Large financial institutions that accept high volumes of remotely deposited checks are especially vulnerable.

- **Mule accounts are also used to facilitate check fraud.** Accounts used to facilitate check fraud are frequently opened at large institutions. Community banks are concerned that these accounts are opened with minimal verification. Stronger enforcement of the Bank Secrecy Act's KYC/CIP requirements would help limit the proliferation of mule accounts.
- **A resolution process could more effectively resolve interbank disputes.** An appropriately tailored resolution process could provide more standardized, timely, and effective resolution of interbank disputes. This would enable community banks to pursue check fraud claims much more efficiently, increasing certainty across the ecosystem.
- **Regulation CC should clarify liability standards.** Regulation CC should explicitly define liability allocation for specific fraud scenarios, particularly for altered checks and forged endorsements. Clear definitions would help level the playing field for community banks and large financial institutions that currently exploit ambiguous rules to shift losses to community banks.

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

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?

- **Fraudsters have kept up with technology enhancements.** While technology enhancements could enable faster funds availability, criminals have matched or exceeded any benefit of these advantages with their ability to alter checks in almost undetectable ways. As a result, financial institutions need even more time to verify the validity of checks than even a few short years ago.
- **Shortening hold times would have negative effects.** Shortening hold times across the board would limit banks' ability to effectively detect and mitigate check fraud by reducing the amount of time banks have to review checks. As a result, all businesses and consumers—including underbanked and lower-income consumers—would continue to suffer losses from check fraud.
- **Extend hold times under appropriate circumstances.** Regulation CC should allow longer hold times for mobile check deposits or under other appropriate circumstances, including, for example, new accounts or accounts that display certain usage patterns. Providing additional flexibility to hold funds would provide significantly greater opportunity to identify suspected payments fraud.



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 “reasonable cause to doubt collectability” exception should be clarified.** The existing “reasonable cause” standard is vague and creates uncertainty for community banks. While this is a valuable exception, clearer guidance would help increase community banks’ confidence in invoking the exception. A safe harbor that would apply when certain conditions are met would also encourage community banks to invoke the exception.

Payments Fraud Data Collection and Information Sharing

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

- **Create a centralized data repository.** The joint regulators could create a single fraud data repository that is accessible to all financial institutions at no cost. The data repository could include historical fraud information, as well as real-time fraud intelligence that would provide all financial institutions with actionable information.

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 and antitrust concerns limit information sharing.** Community banks are often concerned that sharing data about customers with other financial institutions could create liability or otherwise violate existing policy. Clear guidance with concrete examples for community banks could encourage information sharing. A safe harbor that would apply when certain conditions are met could also encourage financial institutions to share useful data.
- **Data collection and sharing impose costs on community banks.** Community banks face resource constraints that make it difficult for them to adopt or implement fraud information sharing capabilities. Community banks would benefit from automated data collection, analysis, and reporting tools that are integrated with services they already use and do not come with additional costs.



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?*

- **Explain how the classifier models could be applied by community banks.** The FraudClassifier and ScamClassifier models have significant potential to standardize payments fraud data. Community banks would benefit from specific instruction on how to implement the classifier models as part of their operations.

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?*

- **Check image verification data is the most urgent need.** A database of check images that have been identified as fraudulent would prevent duplicate deposits and help financial institutions to identify altered checks. The FRS is best positioned to collect and share this data because of its role in the check clearing process.

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?*

- **Centralized databases or repositories are important.** Providing a single source of data accessible to all financial institutions would enable the ecosystem leverage the same information to prevent, detect, and mitigate fraud in all its forms. In addition, it would help to create a level playing field where smaller institutions would not be shut out of accessing more sophisticated, costly data.
- **The FRS is best positioned to develop a centralized database or repository.** The FRS already plays a key role in the payment system and has a strong history of effective product development and delivery. The FRS can also ensure equal access for all financial institutions.

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?*

- **Require fraud reporting across payment rails.** The FRS should require fraud reporting for ACH, wire, and check, like FedNow. Requiring fraud reporting would provide a rich source of data that financial institutions could use to detect and prevent



fraud. However, the FRS should take care to minimize the reporting burden on community banks by integrating and automating the functionality as much as possible.

- **Provide appropriate pricing for community banks.** Fraud products and services offered by the FRS should use pricing that is appropriate for community banks' size and complexity. Community banks face resource constraints that can prevent them from implementing advanced fraud detection and prevention tools and technologies.

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?*

- **Community banks would benefit from a variety of additional risk management tools and services.** A payments fraud contact directory for financial institutions, tools that can provide notification of atypical payment activity, and a confirmation of payee service would all help community banks prevent, detect, and mitigate fraud.

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?*

- **Check fraud harms community banks and their customers.** Community banks and their customers continue to be challenged by a rise in fraud and scams across payment types. Most significantly, check fraud has emerged over the past several years as a leading concern. Mail theft, increasingly sophisticated mechanisms for altering paper checks and check images, and coordination problems among financial institutions have led to mounting losses for community banks.
- **Other fraud and scam mechanisms are of increasing concern.** Community banks are also facing a variety of other threats, including, for example, first-party fraud, elder fraud, and authorized push payment scams like business e-mail compromise. Many of these threat vectors have potential to be further weaponized using artificial intelligence.

26. *Are there specific actions that commenters believe could encourage the use of payment methods with strong security features?*

- **Incentivize movement from paper checks to electronic payments.** Community bank customers are generally ready to send and receive electronic payments, but a small number of customers still rely on checks, especially to send payments, because of infrastructure limitations. The joint regulators should focus on easing and encouraging the transition for these consumers and small businesses.



Thank you for the opportunity to provide comments on this RFI. ICBA looks forward to continuing to work with the OCC, FRB, FRS, and FDIC, and other stakeholders, to protect our communities from the persistent threat of payments fraud. Should you wish to discuss our comments in further detail, please feel free to contact Scott Anchin at [REDACTED]

Sincerely,

/s/

Scott Anchin
Senior Vice President, Strategic Initiatives and Policy

[REDACTED]