[redacted]

From: Stephanie Bliga <[redacted]>
Sent: Thursday, July 31, 2025 8:40 AM
To: Comments
Cc: Robert Voets
Subject: [EXTERNAL MESSAGE] June 20th, 2025 - June 20, 2025 - Request for Information on Potential Actions To Address Payments Fraud; Comment Request (RIN 3064–ZA49)
Attachments: FIL 23-2025 Response.pdf

[redacted]

Good morning,

Please see the comments attached, completed by Ion Bank's VP, Financial Crimes Investigations and Fraud Intelligence Unit, Robert Voets.

Thank you,

Stephanie Bliga
FVP, Risk & Compliance Officer
[redacted]
www.ionbank.com

[redacted]

1. **How can collaboration among stakeholders be improved to combat payments fraud?**
   Establishing regional fraud task forces that include financial institutions, law enforcement, and technology providers. These forums would facilitate timely information sharing and coordinated responses to emerging threats.

2. **What types of collaboration (e.g., standard setting) are most effective, and what are the obstacles?**
   Standardized fraud typologies and reporting formats are most effective. Obstacles include inconsistent definitions and limited resources to participate in national initiatives as well as nationwide information sharing under a safe harbor.

3. **Which non-financial organizations could contribute meaningfully to fraud detection and prevention?**

   Telecommunications companies, social media platforms, and cybersecurity firms can provide valuable insights into scam origination and propagation.

4. **How could increased collaboration among federal and state agencies help?**
   Improved coordination can streamline reporting requirements and enforcement actions, reducing duplication and confusion for community banks.

5. **What types of fraud education are most effective, and should they differ by audience?**
   Scenario-based training and real-life case studies are effective. Education should be tailored—simplified for consumers and more technical for business clients.

6. **Would more education on safe payment practices help reduce fraud?**
   Yes. Proactive nationwide education campaigns can significantly reduce susceptibility to scams, especially among vulnerable populations.

7. **How can existing education efforts be improved or better targeted?**
   Partnering with local schools, senior centers, and chambers of commerce can help reach key demographics but in smaller groups. A nationwide effort has to be exerted on all fronts, from grammar schools on up. Each generation has to be exposed to this education in a cost-effective manner.

8. **Are current online resources effective? If not, how can they be improved?**
   Many are underutilized. Centralizing resources on a single, user-friendly platform with multilingual support would improve accessibility but does not

guarantee use, it attitude of I am too smart for that, or it only happens to other people has to be changed.

9. **What regulatory changes (excluding Regulation CC) could help mitigate payments fraud?**

   Clarifying liability in authorized push payment fraud and encouraging adoption of secure authentication methods would help. There also needs to be an overhaul of UCC.

10. **Is current supervisory guidance sufficient? If not, what should be added or revised?**

    More specific guidance on fraud risk management expectations for small institutions would be helpful. More scrutiny of larger banks and their failure to pay Breach of Warranty claims should be done.

11. **How could new guidance help small community banks?**

    Tailored guidance can help prioritize limited resources and adopt scalable fraud controls.

12a. How often do holds occur, and how responsive are institutions?

The current rules for holds and cash like items need to be revamped. Community banks strive to be responsive, but clearer rules would help manage customer expectations.

12b. Are current disclosures adequate, or should SAR confidentiality rules be revised?

Disclosures could be improved. Allowing limited disclosures without violating SAR rules would enhance transparency.

12. **What challenges do institutions face in resolving interbank disputes over fraudulent checks?**

    Lack of standardized processes and delayed responses from counterparties complicate resolution. Smaller banks are constantly being told by larger banks that a check is not Altered but instead counterfeit or it is counterfeit because it was washed and the makers signature was somehow replaced or traced with no regards to what UCC says; only options is to take civil action which the larger banks know will not happed as it is too expensive.

14a. Have tech advances reduced the need for long hold times?

Yes and no, an "ideal" hold time would be 3 day to give the paying bank time to dishonor the item without loss to the BOFD.

14b. What would be the impact of shorter hold times?

It could greatly increase fraud losses unless paired with enhanced detection tools which would also result in increased costs.

14c. Should the expeditious return requirement be revised?

Yes. Allowing more time for investigation in suspected fraud cases would be beneficial.

13. **Is the "reasonable cause to doubt collectability" exception effective? Should it be clarified?**
    It is useful but needs clearer criteria to ensure consistent application.

14. **How can fraud data collection and sharing be improved?**
    Creating a centralized, anonymized fraud database accessible to all banks would be valuable with information being able to be "digested" in fraud analytics tools and have it for all payment types.

15. **What barriers exist to data sharing, and how can they be overcome?**
    Privacy concerns and lack of standard formats. Regulatory safe harbors and templates could help.

16. **What role should the agencies play in standardizing fraud data?**
    Agencies should lead efforts and funding to define common data elements and reporting protocols.

17. **What types of data would be most impactful, and who should collect/share it?**
    Data on fraud typologies, loss amounts, and recovery rates. Agencies and industry consortia could manage collection.

18. **Is there a need for centralized fraud data repositories? What are the risks and who should manage them?**
    Yes. Risks include data breaches and misuse. A neutral third party under regulatory oversight should manage it.

19. **How can Reserve Banks enhance their fraud risk tools and services?**
    Provide real-time alerts, anomaly detection, and fraud trend dashboards to participating banks.

20. **What new tools or services should be considered (e.g., fraud contact directories, anomaly alerts, confirmation of payee)?** All of the above.
    Confirmation of payee would be especially helpful in preventing misdirected payments.

21.What types of fraud most affect your organization, and what tactics are used?

Check fraud and romance scams. Tactics include social engineering and forged or altered documents stolen from the mail.

22.What measures have been most effective in combating fraud? What can consumers do to help?

Multi-factor authentication, transaction monitoring, and customer education. Consumers should verify requests and report suspicious activity.

23.Are there other actions not yet discussed that could help mitigate fraud?

Encouraging adoption of secure payment rails and incentivizing fraud reporting would help.

24.What could encourage the use of more secure payment methods?

Fee reductions, faster settlement, and fraud protection guarantees would drive adoption.