From: Sally Myers
To: Comments
Subject: [EXTERNAL MESSAGE] June 20th, 2025 - June 20, 2025 - Request for Information on Potential Actions To Address Payments Fraud; Comment Request (RIN 3064–ZA49)
Date: Monday, August 4, 2025 2:12:07 PM

[redacted]

1. **What actions could increase collaboration among stakeholders to address payments fraud?**
    - A regular forum through which we could freely exchange data on fraud experiences across channels (ACH, Debit Card, (perhaps like a 314(b) process) where the community could readily access information regarding potential or suspected fraud.
    - Proactive Regulatory guidance on expectations. This would standardize the industries' approach somewhat to be able to communicate more effectively.

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?**
    - Modernize Reg E to address the current payments and fraud landscape including an alignment with card issuers specifically MasterCard and Visa. Currently, there are various rules etc. that apply to an electronic payment based on the mode of payment (ACH, Debit Card). This makes monitoring and resolving fraud increasingly difficult.
    - Clarifying guidance on regulatory expectations surrounding bank liability when the customer gives out information. Clearer lines between a valid claim and a customer loss.
    - Stronger rules in charging back payments to the merchants instead of Banks bearing the weight.
    - Fines for merchants that have not upgraded to a tap feature for debit cards. This can be passed through the banks.
    - Full disclosure of the merchant name that is responsible for the compromised debit card instances.
    - A database or something similar that contains fraud information (names, addresses etc.) that could be accessed through an online lookup function similar to an OFAC lookup. This would contain national and international data.
    - Stronger guidance on managing risks surrounding the common channels through which fraud is filtered mainly crypto companies. Maybe a reserve account or some sort of mitigation for payment to fraud victims or their banks within a period of time.
    - The big banks and other "coinbase/crypto" players seem to have a large

number of the actual accounts that fraudsters use to funnel the money from our banks to the fraudsters- they need to be defined by number of fraudulent transactions and looked at for tighter account opening due diligence- I hate to bring this up because it could cause more stringent guidance for community banks also but I do not think that all banks are putting the effort in to due diligence of accounts.

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?**
    - Technology giants i.e. Apple, Amazon, Google
    - Digital Currency Companies
    - Fintech Companies and other Cash App creators
    - Large Retailers i.e. Walmart, Target
    - Third party funds transfer systems

4. **Could increase collaboration among Federal and State agencies help detect, prevent, and mitigate payments fraud? If so, how?**
    - Yes, we feel that the regulators, law enforcement and government agencies may all have their own approaches to identifying and mitigating fraud, however, the separations create delays which allow the fraudsters to be much more nimble etc. Perhaps an interagency fraud group similar to the FFIEC. Additionally, this group would produce standardized guidance.

Sally Myers

Senior Executive Vice President, Deputy Chief Risk Officer

Longview Greggton

[redacted]