[redacted]

From: Paine, Tiffany <[redacted]>
Sent: Monday, September 8, 2025 12:09 PM
To: Comments
Subject: [EXTERNAL MESSAGE] June 20, 2025-Request for Information On Potential Actions To Address Payments Fraud; Comment Request (RIN 3064-ZA49)

[redacted]

Ms. Jennifer M. Jones
Deputy Executive Secretary
Attention: Comments—RIN 3064-ZA49
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

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

My name is Tiffany Baer Paine from Security Bank USA in Bemidji, MN. We are a $250MM bank in a small town in Northern MN.

Unfortunately, this is going to be a record year for us when it comes to fraud losses. We have experienced Check Fraud, ACH Fraud, Debit Card Fraud, attempted Wire Fraud and a BIN attack. As you can imagine, this has created stress on our limited resources.

- We have purchased software and added staff.
- We and are planning to add more staff to monitor / mitigate risk for the bank and our customers.
- We regularly communicate with our customers to help educate them on fraud and how to protect themselves.
    - Ultimately, the customer is inconvenienced but not out any money. This does not create as much urgency on their part.

The following is a breakdown of some **opportunities** for action as I see it:

🟦 **Joint Opportunities (OCC, FRS, FDIC Collectively)**

1. Unified Fraud Reporting and Monitoring Framework

- **Create a centralized fraud data-sharing system** where banks report fraud trends (e.g., check fraud, business email compromise (BEC) in wires, real-time payment scams).
- Improve **inter-agency coordination** on fraud typologies and responses.
- Facilitate **real-time fraud alerts** across institutions and regulators.

2. Collaborative Guidance & Best Practices

- Issue **joint guidance** on:
    - Fraud detection technologies (e.g., AI/ML for transaction monitoring).
    - Customer authentication standards (e.g., multi-factor authentication).
    - Vendor risk management in payment processing.
- Promote **standardized protocols** for fraud prevention across all payment rails.

3. Industry Engagement & Public Education

- Host joint forums, roundtables, and webinars with financial institutions, fintechs, and consumers.
- Launch a **national consumer education campaign** around payment fraud risks and how to prevent them (e.g., scams in instant payments).

4. Encourage Adoption of Secure Standards

- Support transition to:
    - **Image-based check clearing** with fraud detection overlays.
    - **ISO 20022** for richer payment data and better fraud screening.
    - Secure instant payment platforms (e.g., FedNow, RTP) with built-in fraud mitigation.

🏛️ **OCC-Specific Opportunities**

As the **primary regulator for national banks**, the OCC can:

1. Enhance Supervision on Fraud Controls

- Intensify examination focus on banks' payment fraud risk management practices.
- Require national banks to implement enhanced due diligence for high-risk payment channels.

2. Promote Use of Advanced Technology

- Encourage supervised banks to adopt AI/ML fraud detection systems and anomaly-based alerting for wire and ACH payments.

🏛️ Federal Reserve System (FRS)-Specific Opportunities

As both **regulator** and **payments operator** (e.g., ACH and Fedwire), the FRS can:

1. Strengthen Payment Infrastructure

- Enhance **Fedwire and FedACH fraud controls**, including:
    - Pre-validation of account numbers.
    - Behavioral transaction scoring.
- Expand **FedNow fraud tools** to support bank-level mitigation (e.g., transaction limits, velocity checks).

2. Operational Collaboration

- Collaborate with financial institutions to **pilot anti-fraud APIs** or tools (e.g., account name matching on FedNow).
- Provide **fraud simulation environments** for banks to test controls.

🛡️ FDIC-Specific Opportunities

As the **insurer and supervisor** of many state-chartered banks, the FDIC can:

1. Risk Management for Community Banks

- Offer tailored guidance to **community banks**, which may lack fraud-fighting infrastructure.
- Launch **technical assistance programs** to help smaller banks adopt fraud mitigation tools.

2. Deposit Insurance and Consumer Protection Focus

- Clarify **reimbursement expectations** and protections for consumers scammed via faster payments.
- Work with banks to **balance fraud mitigation with inclusion** (avoid de-risking).

🔍 Potential Focus Areas by Payment Type

Payment Type	Risk	Regulatory Actions
Checks	Counterfeit, alteration, kiting	Promote image analysis tech, enhance back-office controls

ACH	Account takeover, unauthorized debits	Advocate for account validation tools, tighter originator due diligence
Wires	BEC, impersonation	Encourage real-time fraud scoring, hold-and-verify protocols
Instant Payments	Authorized push payment (APP) scams	Require strong customer authentication, consider optional delays for suspicious transactions

---

Thank you for your time.

Tiffany Baer Paine

SECURITY BANK[USA]

Tiffany Baer Paine

President / Co-CEO

Board of Directors

Phone: [redacted]

Cell: [redacted]

Fax: [redacted]

[redacted]

For the **safety of your confidential information**,

Security Bank[USA] may encrypt and send your e-mail via **ZIX**.

If you have any questions, please contact your banker at [redacted].

Here for good.

Try our Mobile Banking App!

Visit Us @ www.SecurityBankUSA.bank