From:	Martin Haggard
To:	Comments
Subject:	[EXTERNAL MESSAGE] June 20, 2025-Request for Information On Potential Actions To Address Payments Fraud; Comment Request (RIN 3064-ZA49)
Date:	Friday, September 19, 2025 11:32:49 AM

[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:

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:

I am the President/CEO of Wayne County Bank (Bank), a $568MM community bank

located in Waynesboro, TN. I am writing to 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.

Wayne County Bank is a community bank based in Waynesboro, TN. Founded in 1914, we've grown to $568MM in total assets and 8 locations throughout 3 counties. We offer a full suite of banking products and services, including a variety of deposit accounts and personal and business loan products. Our core focus is small business loans (SBL), which are loans to SBs and farms for C&I activities and Ag.

Wayne County Bank takes pride in still having the friendly personal touch that has been our hallmark when we began in 1914. Today, our staff still know most of their customers on a first name basis, and the bank is stronger and more secure than ever. We pride ourselves on our personalized approach to community banking and our commitment to and deep roots in the communities that we serve.

I applaud 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.

Specifically, the Bank has been affected by payments fraud in the following ways:

- Person-to-Person transfers reported as fraudulent where the bank has to recourse and must assume the loss.
- Mobile Deposits where funds are withdrawn from ATM.
- ATM Deposits that are not valid checks but may have been done after hours and funds were withdrawn before the check(s) could be reviewed.
- Gift Card purchases where customers send fraudsters the code and they claim the funds.
- Digital Currency ATMs where cash is converted to a Digital Currency.

External Collaboration

The Bank supports collaborative stakeholder efforts to address payments fraud. Fraud and scams persist across state borders, so national stakeholder collaboration is necessary to effectively combat the problem. However, national efforts must recognize the resource constraints individual community banks face when deciding whether to participate.

- 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.

Consumer, Business, and Industry Education

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

Regulation and Supervision

- Broadly speaking, payments fraud regulations and examiner expectations need to be appropriately tailored to community banks with tiered compliance requirements and deadlines. There are opportunities to enhance supervisory guidance around appropriate controls, suitable technology, reporting, and incident response, but it is important to avoid imposing new burdens on community banks.
- Changes to Regulation CC could help community banks prevent and mitigate check fraud. For example, the return deadline related to fraud could be extended, the "reasonable cause to doubt collectability" exception could be clarified, and relevant definitions could be revised (e.g., "altered" and "alteration"). However, hold times should not be shortened; they are an essential tool for banks to detect and prevent check fraud. Financial institutions should have flexibility to extend hold times under appropriate circumstances.

Payments Fraud Data Collection and Information Sharing

- While centralized data reporting would be valuable for the ecosystem, agencies should avoid imposing additional data collection requirements on community banks. Appropriate safe harbors would improve banks' ability and willingness to share fraud data.
- 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.

Reserve Banks' Operator Tools and Services

- Community banks would benefit from tools and services that integrate with third-party services they already use and pricing that is appropriate for their size and complexity.
- There are a variety of specific products and services that could benefit community banks, including, for example, a fraud contact directory, a fraud information sharing repository, an interbank check fraud breach of warranty claim mechanism, a check image analysis and verification tool, an atypical payment monitoring service, and confirmation of payee service.

General Questions

- Person to Person (P2P) Payments where a customer may be coerced into sending a payment to a fraudster in relation to back taxes, financial assistance, investment opportunities, ect. These payments are reported to the bank as fraud and the Bank does not have recourse to recoup these funds due to the payment network type and being consumer initiated. Fraudsters have also coerced customers into allowing access into their personal devices in which they may assume control and initiate a payment themselves while the customer is not fully aware of what is happening.

- Mobile Deposit Scams are an increasing issue with customers attempting to get online loans, employment, and investment opportunities. Fraudsters are

presenting as Loan Companies, Employers, and Investors that require Online Banking credentials in order to make a “Direct Deposit” to a customers account. These types of deposits are typically checks that have been stolen from the mail and reproduced with altered information or generically created that may look legitimate at first glance.

- ATM Deposits have started to arise shortly after the Mobile Deposit scams. These are deposit that are typically not valid checks but may have been done after hours and funds were withdrawn before the check(s) could be reviewed. Fraudsters may use a variety of methods, similar to Mobile Deposit Scams, and inform customers they should go after hours or not to discuss details with their Financial Institutions. They will attempt to manipulate the customer into believing that the bank is against them and it is better to use the ATMs.

- “Love Scams” where Fraudsters manipulate and convince customers (primarily targeted at the elderly) that they are in love with them and need money to get to them or for a family emergency. Often Fraudsters will impersonate celebrities and have been utilizing AI to generate realistic pictures and voice calls. Payment methods such as wires, P2P Transfers, and Gift Card purchases are utilized. The customers are willingly sending these payments and cannot reclaim their funds. The

- We have employed internal controls and reviews with personnel versed in Fraud Management. Training is provided in relation to these controls and reviews, as well as effective communication regarding newly trending scams and current instances of scams we personally see.
- Frontline personnel are trained to pay attention to their customers and the deposit. Making a friendly approach to a customer and efforts to know customers has proven to be beneficial for detecting fraud.

Thank you for the opportunity to provide comments on this RFI. The Bank looks forward to continuing to work with the OCC, FRS, and FDIC, and other stakeholders to protect

our customers and communities from the growing threat of payments fraud.

Sincerely,

/s/

Martin L Haggard, Jr

President/CEO

Wayne County Bank