Via electronic mail

September 18, 2025

Federal Deposit Insurance Corporation
550 17th Street NW
Washington, D.C. 20429
comments@FDIC.gov

Re: RIN 3064-ZA49;
Request for Information on Potential Actions to Address Payment Fraud

On behalf of Hancock Whitney Bank, we appreciate the opportunity to respond to the interagency Request for Information (RFI) on payments fraud, an important topic not just for financial institutions but for our customers. While we are highly encouraged by the interagency focus on this issue, which is impacting millions of Americans, we also believe Congressional action is needed to support these efforts. For that reason, earlier this year, we and other large Mississippi based banks sent the attached letter to our Congressional delegation as well as the Senate Banking Committee and House Financial Services Committee urging them to continue to focus on this very important issue through the adoption of a multi-stakeholder approach.

In addition to the recommendations we made in our prior letter, we also strongly support the positions taken by the American Bankers Association (ABA) in response to the RFI. We believe the ABA's recommendations offer a practical and comprehensive approach to addressing fraud across the financial ecosystem.

Payments fraud poses a complex and widespread threat impacting consumers, businesses, and financial institutions alike. The complexity of fraud schemes means that banks alone cannot solve this problem. It requires a coordinated, muti-stakeholder approach. In alignment with the ABA's recommendations, we offer the following comments to reinforce and expand upon their proposals.

Shared Responsibility to Prevent Fraud

Most scams originate outside of the banking payment system—on platforms such as social media, telecom networks and search engines. Banks cannot prevent fraud that originates beyond their control. We support the ABA's recommendations to implement upstream interventions that prevent scams from reaching customers and stopping them before they enter the payment system, including:

- Establishing a centralized Federal Office of Fraud Prevention to coordinate fraud prevention efforts.

- Promoting responsibility among telecom providers, social media platforms, and internet search engines to identify and block fraudulent content.
- Encouraging collaboration with telecoms and tech platforms since they have data and play an important role in scam origination.
- Creating safe harbors to assist with cross-industry data sharing.

Regulatory Considerations

Any regulatory guidance on this issue must be clear and actionable. For example, while Regulation CC plays a critical role in preventing fraud, the current framework does not adequately reflect the speed and sophistication of modern fraud schemes, and delays in confirming fraud can result in irreversible losses. Regulation CC should be updated to include a fraud exemption allowing banks to place holds based on internal indicators of fraud. In addition, any regulatory guidance should be tiered to take into consideration the operational constraints of small, mid-sized and large financial institutions.

We support the ABA's recommendations for:

- Providing consistency for regulatory guidance and exam expectations.
- Recommending detailed supervisory guidance tailored to a bank's size and risk profile.

Enhanced Fraud Prevention Education

Coordinated and consistent messaging builds public trust and awareness that enables both consumers and small businesses to recognize threats to their financial security. Therefore, we support efforts to expand consumer and business education, especially for vulnerable groups such as seniors and small business owners, to help prevent fraud, which includes:

- A task force model to align education efforts ensuring consistent effective messaging to avoid contradictory information reaching consumers and businesses.
- Centralized messaging ensuring consistency and credibility across all banks.
- Education that focuses on emerging threats.

Conclusion

Banks remain committed to protecting consumers and businesses, but a unified, cross-sector response is required to stop fraud before it starts.

We respectfully request that the FDIC and other agencies consider the recommendations outlined in our June 18, 2025 letter and adopt the ABA's proposals to establish collaboration and accountability to tackle fraud.

Thank you for allowing us the opportunity to comment on this important topic. We hope to have continued discussions and are eager to support efforts that protect Americans from financial harm.

Respectfully submitted,

Hancock Whitney Bank
Gulfport, Mississippi

June 18, 2025

Via Email and US Mail

Senator Roger Wicker
425 Russell Senate Office Building
Washington, D.C. 20510

c/o Julia Wood - [redacted]
and Beth Spivey – [redacted]

Senator Cindy Hyde-Smith
528 Hart Senate Office Building
Washington, DC 20510-2405

c/o Doug Davis – [redacted]
and Hayes Heredia [redacted]

Subject: Protecting Americans from Fraud and Scams

Dear Mississippi Senate Delegation:

Millions of Americans are being targeted by sophisticated fraud schemes resulting in significant financial losses and emotional distress. Bankrate's latest Financial Fraud Survey found that about one in three adults have experienced a financial fraud or scam in just the last 12 months, while nearly two in five among them have experienced a financial loss.[1] The vast scale of this problem means it is difficult to identify comprehensive numbers, but in 2023, the FTC estimated fraud losses affecting Americans to be as high as $158.3 billion.[2] These scams often originate through text messages, emails, or social media, exploiting advanced technologies like artificial intelligence and voice cloning to deceive individuals.[3]

[1] https://www.bankrate.com/credit-cards/news/financial-fraud-survey/#:~:text=More%20than%202%20in%203,sent%20funds%20to%20a%20scammer

[2] https://www.ftc.gov/system/files/ftc_gov/pdf/federal-trade-commission-protecting-older-adults-report_102024.pdf ("In 2023, the FTC estimates the overall loss, adjusted for underreporting, was $158.3 billion or $23.7 billion for consumers of all ages and $61.5 billion or $7.1 billion for older adults. These estimates are based on two different assumptions about the degree of underreporting for high dollar losses.")

[3] National Consumer Protection Week: What You Need to Know About Artificial Intelligence Scams, NYC Consumer and Worker Protection (March 7, 2024), https://www.nyc.gov/site/dca/news/014-24/national-consumer-protection-week-what-you-need-know-artificial-intelligence-scams

While banks have implemented secure efficient payment platforms and products that safeguard financial transactions, we cannot control external platforms where fraud begins.[4] We are asking Congress to conduct additional hearings to explore the origins, far-reaching impacts, and action steps necessary to address this fraud epidemic. Protecting Americans requires a whole of government, multi-stakeholder approach with telecom providers, social media platforms, and internet search engines stepping up to detect and block fraud at its source. Addressing this issue requires a collective effort by the government and private industry, and immediate action is needed to shield Americans from this persistent threat.

The Human Toll of Fraud and Scams:

The victims of fraud are not just statistics—they are everyday Americans. Imagine a retiree unknowingly transferring their life savings to a scammer posing as their bank, or a young couple losing a rental deposit to a fake landlord they found online. These scams leave not only financial devastation but also lasting emotional scars eroding trust in the digital tools that are becoming essential to daily life.

The financial losses for Americans are staggering.

- Imposter scams: In 2024 the FTC reported that about 1 in 5 people lost money to impostor scams, where fraudsters impersonate legitimate businesses or individuals to deceive victims, with reported losses at nearly $3 billion dollars and a median loss of $800.[5]
- Romance and Investment scams: The FBI has reported that investment scams, which many times are part of a romance scam, are the fastest growing fraud with $6.5 billion in losses reported in 2024.[6] Many of these fraud schemes originate from foreign countries where fraud rings operate at scale using imprisoned people.[7,8]
- Tech Support scams: In 2024, over 36,000 Americans reported losing nearly $1.5 billion in tech support scams where scammers pose as fake representatives of Microsoft or other technology vendors and sell fake fixes or extort their victims, many of them elderly or vulnerable adults, for exorbitant sums of money.[9]

While banks have implemented secure efficient payment platforms and products to facilitate financial transactions, these scams begin outside of the bank's payment network. Scammers hide their true identities in part by spoofing the good names and reputations of banks and other responsible companies. In fact, the FBI in their recent 2024 Internet Crime Complaint report had

[4] Statement for the Record on Behalf of the American Bankers Association, Bank Policy Institute, Consumer Bankers Association, and National Bankers Association, Before the Permanent Subcommittee on Investigations of the U.S. Senate Committee on Homeland Security and Governmental Affairs (May 21, 2024), https://consumerbankers.com/wp-content/uploads/2024/07/Joint-Statement-for-the-Record_July-23-Hearing_Permanent-Subcommittee-on-Investigations.pdf

[5] https://public.tableau.com/app/profile/federal.trade.commission/viz/ConsumerSentinel/Infographic

[6] https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

[7] Emma Fletcher, Romance Scammers' Favorite Lies Exposed, https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed, (February 9, 2023).

[8] Feliz Solomon, The Slaves Sending You Scam Texts - The Journal. - WSJ Podcasts, July 29, 2024

[9] https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

"Phishing/Spoofing" as the number one complaint with 193,407 complaints received over twice as high as the next complaint category of extortion. Fraud necessitates intervention before payments are initiated—in fact, before fraudulent and spoofed communications ever reach Americans.[10,11]

A Call for Shared Responsibility:

Protecting Americans from fraud requires action from all stakeholders. Government must partner with the private sector to lead a whole-of-government response. Combating fraud is a shared responsibility:

1. The government must take the lead on a whole of ecosystem response and should develop a National Fraud and Scam Prevention Strategy and designate an official to lead the overall effort.
2. Telecom providers must be held accountable and fined when they allow spoofed caller ID names and numbers; they need to monitor and block fraudulent calls and text messages at their source before they can reach innocent Americans; and they should create a database from customer reported scam/fraud/junk texts that registered companies could access to identify when their brands are being impersonated to allow them to proactively shut down the scams.
3. Social media platforms must enhance algorithms to identify and shut down fraudulent accounts and create simple and free processes for individuals and brands to report when their names, images and likenesses are being impersonated and have those accounts promptly shut down.
4. Internet search engines must ensure scam websites are flagged or removed.
5. The government must increase information sharing. Banks need updated information from the government on ever-evolving fraud schemes, and well as the latest law enforcement priorities.
6. Bank Secrecy Act rules must be subject to smart, data-driven reform to streamline reporting requirements and allow banks to adopt a true risk-based approach, focusing compliance resources on the real bad actors, and away from check-the-box exercises.

The rapid movement of funds combined with the technological savviness of fraudsters has outpaced the capacity of banks to use existing tools to fully protect Americans. We cannot prevent Americans from receiving fraudulent texts or emails, despite our commitment to safeguard them. Banks continue to invest in advanced security features; however, banks are not the front line of this fraud. We tell our customers to only send money to people they know and trust, but by the time they're ready to make a payment they believe they know and trust who they're sending the money too. The stakeholders that have the tools to prevent these criminals from contacting and building trust with our customers must become an active part of the solution to protect Americans.

[10] P2P Payment Fraud is on the Rise: How To Combat It, September 5, 2024, https://www.pcbb.com/bid/2024-09-05-p2p-payment-fraud-is-on-the-rise-how-to-combat-it

[11] Mike Cetera, Peer-to-Peer Fraud Statistics, **Forbes Advisor** (November, 2024), https://www.forbes.com/advisor/money-transfer/peer-to-peer-fraud-statistics-in-year/

The American public needs responsible safeguards requiring telecom providers, social media platforms and internet search providers to proactively detect and mitigate fraud and scams at the source. Just as post-9/11 reforms helped banks focus on detecting terrorism funding, more must be done to fight the fraud epidemic targeting Americans' life savings. Implementing these safeguards will not be easy or without costs. When the banks acted in concert with the government to follow the money and cut off terrorist funds to protect Americans from the existential threat of terrorism, banks innovated new solutions, and this critical partnership helped turn the tide. Without a collective and shared responsibility, Americans remain vulnerable to sophisticated and life altering scams.

Protecting Americans:

Our main objective continues to be the protection of Americans from life altering disruption and financial loss, and we will continue to do everything in our power to accomplish that objective. However, success is attainable only if responsibility is placed on the appropriate parties at the right stages of these crimes.

Every scam begins somewhere outside of the secure payment system, and every American deserves protection. Stopping these scams cold before they enter the payment system and materialize into financial losses for innocent Americans is the right place to focus. We urge Congress to take swift action by implementing a multi-stakeholder approach that ensures responsibility is placed where it can have the greatest impact. Only through collaboration can we create a safer digital and financial payment environment for all Americans.

Sincerely,

D. Shane Loper
President
Hancock Whitney Bank

Kevin D. Chapman
Chief Executive Officer and President
Renasant Bank

Duane A. Dewey
Chief Executive Officer and President
Trustmark

James D. "Dan" Rollins III
Chief Executive Officer and Chairman
Cadence Bank