Independent Bankers Association of Texas

September 17, 2025

Chief Counsel's Office
Office of the Comptroller of the Currency
400 7th Street SW Suite 3E-218
Washington, DC 20219
Attention: Comment Processing
Re: Docket ID OCC-2025-0009

Ann Misback, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551
Re: Docket No. OP-1866

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

Re: Request for Information on Potential Actions To Address Payments Fraud

Dear Regulators:

This letter is submitted on behalf of the Independent Bankers Association of Texas ("IBAT") a trade association that represents the independent community banks of Texas and the communities they serve.

Introduction:

Payments fraud inflicts significant harm on consumers, businesses, and financial institutions. Payments fraud also has the potential to erode public trust in - and undermine the safety, accessibility, and efficiency of - the nation's payments system, upon which the U.S. financial system depends. As part of their objectives to promote the safety of the U.S. financial system, the FRS, FDIC, and OCC have overlapping but also discrete roles and authorities related to the issue of payments fraud. For example, the Board, FDIC, and OCC all engage in supervision of financial institutions. In addition to supervising financial institutions, the FDIC has the distinct mission to maintain stability and public confidence in the nation's financial system as the insurer of bank deposits.

The FRS, which includes the Board and the Federal Reserve Banks (Reserve Banks), also focuses on payment system safety as a payment system operator and catalyst for payment system improvements.

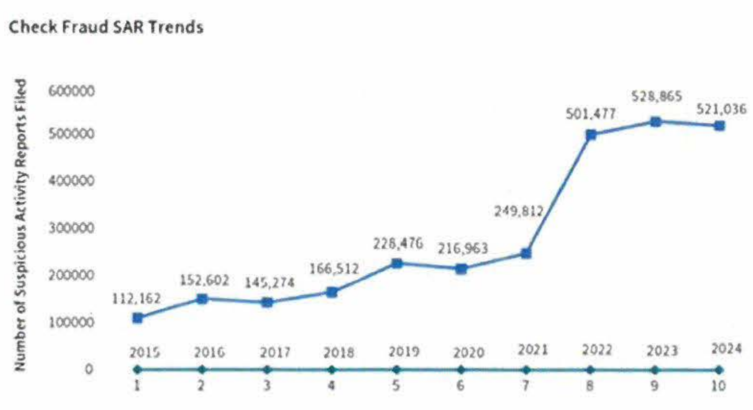
Therefore, the FRS, FDIC, and OCC are each interested in exploring ways to help mitigate risk of payments fraud. Given that the FRS, FDIC, and OCC have specific differing roles and authorities, this mitigation could take the form of collective action where roles align, such as joint supervisory guidance, or independent action where roles differ, such as changes to the payment systems operated by the Reserve Banks.

Background:

In July of 2024, IBAT sent a letter (attached) to the prudential regulators outlining the struggles Texas community banks face with regard to check fraud. Below is an excerpt from that letter.

> *The issue of check fraud is permeating the industry and Texas community banks, and their accountholders are being harmed by this criminal activity. The problem of check fraud is exacerbated by Know Your Customer ("KYC") lapses at the largest institutions that allow fraudulent accounts to be opened – often online with no face-to-face interactions. Our members believe that if the lapses in KYC and account opening were successfully addressed by the Regulators, and solved by the largest institutions, then check fraud would decrease significantly.*
>
> *As check fraud has increased, more than 90 percent of our member banks that responded to our recent survey reported that they have experienced problems in being reimbursed for fraudulent returns in the past year from the bank of first deposit related to breach of presentment warranties.*

We wish we could say the situation has appreciably changed in the last 12 months but, sadly, it has not. That is why we wholeheartedly welcome this request from the agencies for suggestions to address the fraud.



This chart reflects the number of check fraud-related suspicious activity reports (SARs) filed in the last 10 years.
FinCEN data on check fraud is for depository institutions as of February 2025.

The above infographic is from the FDIC's THREAT $POTLIGHT Spring Edition 2025 (attached) that supports our narrative.

Below is an excerpt from our August 2024 letter (attached) to the House Financial Services Committee and Senate Committee on Banking, Housing, and Urban Affairs also highlighting the threat check fraud presents.

> *Check fraud harms everyday consumers and damages the reputations of community banks who truly know their customers. Worse, check fraud is a serious financial crime that aides and abets human trafficking, drug trafficking and terrorist financing.*
>
> *Combating check fraud is analogous to a three-legged stool. The first leg is the customers of the bank, the second leg is the paying bank of those customers, and the third leg is the bank where the check is deposited, also called the bank of first deposit. If each 'leg' is not doing their part to support the system, the system fails. The largest banks, in their role as the bank of first deposit, are often not doing their part in combating check fraud, putting both community banks and their customers at risk.*
>
> *In increasingly sophisticated schemes, thieves and scammers are stealing checks from postal boxes, changing the name of the recipient and the dollar amount on the check, opening fraudulent accounts at a bank, and then hiring someone to deposit the check into an account for them.*
> *Once deposited, the funds are quickly withdrawn from the depository bank before the paying bank becomes aware of the fraud.*
>
> *Thieves and scammers rely on the ability to deposit those fraudulent checks somewhere and that somewhere is usually one of the nation's larger banks. Simply put, the failure of the nation's largest banks to police accounts being opened and the deposits made into those accounts, usually remotely, without adequately addressing 'know your customer' requirements enable the scourge of check fraud to plague our banking system.*

Comments:

1. What actions could increase collaboration among stakeholders to address payments fraud?

Comment: To effectively address payments fraud, collaboration across the financial ecosystem, including banks, financial technology companies, payment processors, law enforcement and regulators is crucial. Establishing a centralized, secure, real-time information sharing platform could help to increase collaboration, as well as provide real-time exchange of fraud typologies, emerging threats and suspicious activity patterns. Current information-sharing efforts (e.g., FS-ISAC and 314(b)) are helpful but often operate on delay or are fragmented or are not targeted at addressing and combatting fraud but rather money laundering and terrorist financing. A centralized system with tiered access levels could allow for more agile threat detection and coordinated responses.

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?

Comment: Payments clear faster than ever and through more channels than ever. While advancements in payments has abounded, the ability for banks to identify fraud and communicate with other banks is lagging behind. Something like Section 314(b) of the USA PATRIOT Act, as mentioned above, that allows banks to share real-time information with each other and to identify and report potential money laundering and terrorist financing activities would be helpful for fraud as well. Notably, the 314(b) program is a voluntary information sharing program and only banks that opt-in participate and must provide a point of contact. Because the program is voluntary, the percentage of banks that have opted-in is low.

The agencies need to develop a fraud communications and reporting framework for all banks that makes participation mandatory. Such a communications platform would 1) allow immediate data collection on compromised account numbers, 2) provide facts on new or developing fraud schemes and 3) provide real-time updates and notifications, giving banks time to act.

As it stands now, by the time the fraud is identified there is no time to act as the money is usually out of the bank of first deposit with little chance to recover any funds absent successfully pursuing a presentment warranty claim. A real-time network would allow all banks to shift from a reactive to a proactive stance, thus better protecting their accountholders. Agencies can also encourage greater participation by including a safe harbor provision for good-faith information sharing, which in turn could lead to open collaboration while maintaining compliance with existing privacy regulations.

4. Could increase collaboration among Federal and State agencies help detect, prevent, and mitigate payments fraud? If so, how?

Comment: We would argue that Federal and State agencies are in fact the only participants that can increase collaboration with banks of all sizes across the country. While the Federal Reserve's Scam Classifier and Fraud Classifier have been helpful, much more is needed regarding shared classification standards, cross agency alerts and guidance on joint training exercises and case studies.

11. How might new or revised supervisory guidance assist small community banks in detecting, preventing, and mitigating payments fraud?

Comment: Similar to the Texas Financial Crimes Intelligence Center, a national unified fraud intelligence center with both reporting and dissemination of information is a critical step that would help consolidate and distribute real-time fraud intelligence to key participants.

13. The Board, FDIC, and OCC have received complaints from supervised institutions regarding challenges in resolving disputes about liability for allegedly fraudulent checks. What is the experience of supervised institutions when trying to resolve these types of interbank disputes regarding allegedly fraudulent checks? Do these types of interbank disputes arise more frequently in connection with certain types of checks or parties? What actions could the Board, FDIC, and OCC consider, including potential amendments by the Board to Regulation CC, that could improve supervised institutions' ability to resolve interbank disputes over liability for allegedly fraudulent checks?

Comment: As noted above, more than 90 percent of our bank members that responded to our survey reported they have experienced problems in being reimbursed for fraudulent returns from the bank of first deposit related to breach of presentment warranties. Our members continue to report problems with the largest banks including Wells Fargo, Bank of America, JP Morgan Chase and Navy Federal Credit Union. More than 60 percent of our member banks have said it has taken more than 6 months on average to get closure for fraudulently returned items.
Improving the communication infrastructure for fund recovery efforts is essential. The current ad hoc process is hindered by inconsistent check return procedures across institutions, particularly when dealing with larger banks. Guidance should be issued to all banks on the proper handling of presentment warranty claims with examples of valid claims and a time frame for resolving claims.

14. Regulation CC seeks to balance prompt funds availability with the risk of checks being returned unpaid for reasons that include fraud. What potential amendments to Regulation CC would support timely access to funds from check deposits while providing depository institutions with sufficient time to identify suspected payments fraud?

Comment: Community banks have been warned by regulators (in particular the FDIC) that they may not place a hold on an account without a legal reason to do so. Even when invoking a 'reasonable cause to doubt collectability' hold under the existing Regulation CC framework (§229.13(e)), the hold must be based on 'the existence of facts' and not just a good faith suspicion of fraud. Additional guidance should be provided to both clarify and expand when a reasonable cause to doubt collectability hold can be placed.

15. Regulation CC provides six exceptions that allow depository institutions to extend deposit hold periods for certain types of deposits, including deposits for which the depository institution has reasonable cause to doubt the collectability of a check. Is this exception effective in allowing depository institutions to mitigate check fraud while also allowing timely access to funds? Would depository institutions benefit from further clarification on when it may be appropriate to invoke this exception? What are the experiences of businesses and consumers when depository institutions invoke this exception in order to delay the availability of depositors' funds?

Comment: Community banks face the ongoing challenge of combating check fraud and other fraudulent activities while complying with Regulation CC's funds availability rules. Expanding the regulatory guidance with careful consideration could potentially limit fraud without placing excessive burdens on accountholders. For example, under a large item hold, (§229.13(b)) the first $6,725 must be made available according to the standard availability schedule, presenting significant risk to the depository bank.

17. What barriers limit the collection and sharing of payments fraud data between industry stakeholders, and how could these barriers be alleviated? For example, have specific barriers limited development of solutions or participation in bilateral or multilateral payments fraud data collection and information sharing? What changes would address these barriers?

Comment: Because of data privacy and liability concerns, the sophistication in phishing and spoofing attempts, resource disparity among banks of varying sizes and potential voluntary participation in any effort, anything other than an agency-led effort would be futile. Banks simply do not share any detailed information via unsecure channels.

18. What role should the FRS, FDIC, or OCC take in supporting further standardization of payments fraud data? For instance, can the FRS better leverage or improve the FraudClassifierSM and ScamClassifierSM models?

Comment: The Federal Reserve System (FRS), FDIC and OCC can play a critical role in advancing the standardization of payments fraud data across the financial industry. Fragmented fraud classification and inconsistent reporting mechanisms limit banks' collective ability to detect trends, respond effectively and benchmark risks. The FraudClassifier℠ and ScamClassifier℠ models provide a strong foundation for improving consistency in fraud categorization. However, adoption remains voluntary and uneven across the industry, just as it does with 314(b) efforts.

Incentivizing or making adoption mandatory by incorporating participation in the models could help with regulatory guidance, understanding examiner expectations or even supervisory frameworks. Also, collaboration is key, not just between banks and the agencies but between all the standard-setting bodies, and while the request for comment has a focus on check fraud, this could assist with other types of payment fraud as well (i.e. NACHA). By expanding the adoption, refinement and integration of the FraudClassifier℠ and ScamClassifier℠ models, agencies can help create a unified framework that enhances fraud detection, reporting and prevention across the ecosystem.

20. Is there a need for centralized databases or repositories for the sharing of payments fraud data across entities? What legal, privacy, or practical risks and challenges could such a centralized database or repository pose? Which entities are best positioned to develop and participate in a centralized database or repository?

Comment: The answer to the initial question seems to be a resounding, 'Yes.' The extended response times allowed between receiving and replying to fraud inquiries introduce unnecessary friction and delay, often hindering timely action. While smaller community banks are doing their best to monitor and respond to fraud internally, their reporting capabilities are limited—typically restricted to filing Suspicious Activity Reports (SARs). This limitation is frustrating and insufficient for addressing the broader scope of the fraud. Without a centralized reporting mechanism, incidents below the SAR reporting thresholds remain disconnected and unrecognized as part of a broader pattern of risks to the industry.

Reiterating the problem, check fraud targets every bank, every consumer and every business in the country. It is a means to funnel money that supports human trafficking, drug trafficking and terrorist financing and it is high time to take serious actions to address the growing concern.

We look forward to any discussions on the rules that would further protect the interests of both Texas community banks, the borrowers and the communities we, as an industry, serve.

Sincerely,

[redacted]

Christopher L. Williston, CAE
President and CEO