September 18, 2025

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

Ms. Ann Misback
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

Ms. Jennifer M. Jones
Deputy Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

Re: Request for Information on Potential Actions to Address Payments Fraud—Docket ID
        OCC-2025-0009; Docket No. OP-1866; RIN 3064-ZA49

To whom it may concern,

On behalf of The American Fintech Council (AFC),[1] I am submitting this comment letter in
response to the Request for Information on Potential Actions to Address Payments Fraud (RFI)
by the Board of Governors of the Federal Reserve (FRB or Federal Reserve), Federal Deposit
Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC)
collectively referred to as the "Joint Agencies".[2]

AFC's mission is to promote an innovative, transparent, inclusive, and customer-centric financial
system by fostering responsible innovation in financial services and encouraging sound public
policy. AFC members are at the forefront of fostering competition in consumer finance and
pioneering ways to better serve underserved consumer segments and geographies. Our members
are also improving access to financial services and increasing overall competition in the financial

---

[1] American Fintech Council's (AFC) membership spans EWA providers, lenders, banks, payments providers, loan servicers, credit bureaus, and personal financial management companies.
[2] Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, "Request for Information on Potential Actions to Address Payments Fraud", Fed. Reg. 90, no. 117 (Jun. 20, 2025): 26293.

1

services industry by supporting the responsible growth of lending and lowering the cost of financial transactions, allowing them to help meet demand for high-quality, affordable financial products.

AFC appreciates the Joint Agencies' efforts to engage in a concerted and pragmatic manner regarding the issue of payments fraud. While AFC recognizes the differing jurisdictions of each of the Joint Agencies, combatting payments fraud is crucial and cross-cutting aspect of ensuring a safe and sound financial services industry that effectively serves consumers. According to the Federal Trade Commission's 2024 Consumer Sentinel Network's 2024 Data Book, "[b]ank transfers and payments accounted for the highest aggregate losses reported in 2024 ($2.09 billion), followed by Cryptocurrency ($1.42 billion), while credit cards were most frequently identified as the payment method in fraud reports."[3] This is not to say that industry participants or regulators are not working diligently to combat payments fraud. Instead, it underscores the clear importance in developing a robust and effective framework for combatting payments fraud.

Payments fraud is far from a new or emerging topic in the financial services industry. Both the Joint Agencies and industry participants have previously pursued substantial efforts to combat payments fraud. For example, FRB launched its FraudClassifier[sm] and ScamClassifier[sm] in 2022 and 2024 respectively. Both of these efforts established voluntary classification structures that financial institutions could use to more easily detect fraud and scams. In addition, as noted by our members and a recent U.S. Government Accountability Office report, financial institutions and fintech companies have pursued significant technological and educational efforts to mitigate fraud risk and proactively root out nefarious actors from the financial services ecosystem.[4] While it is important to note that these activities are not costless, responsible, innovative banks and their fintech partners consistently pursue these efforts in order to mitigate fraud risk to their consumers.

The complexity of combatting payments fraud requires a comprehensive, coordinated, and unified approach by both the Joint Agencies and other relevant regulators that operates in concert with the efforts conducted by industry participants. Payments fraud thrives on exploiting regulatory and market gaps. Payments fraud, like other types of fraud in financial services operates dynamically using time-tested strategies. Sophisticated actors are not simply one-off scammers but instead are often part of a fraud ring that works in a coordinated, organized manner, relying on the lack of transparency and operational inefficiencies within the existing financial services ecosystem. Further, these sophisticated actors leverage the latest technological tools, including generative AI tools and advanced bots, to pursue nefarious activities. Thus, to combat these sophisticated actors, the Joint Agencies must match the organizational and technological capabilities of the nefarious, sophisticated payments fraud actors by pursuing activities that will facilitate the transparent movement and analysis of data throughout the financial services ecosystem.

---

[3] Federal Trade Commission, Consumer Sentinel Network Data Book 2024, Federal Trade Commission, Mar. 2025, Page 4, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf.
[4] U.S. Government Accountability Office, *Payment Scams: Information on Financial Industry Efforts*, GAO-24-107107 (Washington, D.C.: GAO, 2024), *available at* https://www.gao.gov/products/gao-24-107107.

In an effort to improve both government and industry efforts to combat payments fraud, AFC has put forward the below recommendations in response to the questions posed by the RFI for the Joint Agencies consideration.

> **I.** **AFC recommends that the Joint Agencies Pursue a Program that Ensures the Seamless and Transparent Movement of Data of Potential Payments Fraud Activities, and That the Joint Agencies Provide a Positive Feedback Loop on the Data to Improve Industry Practices Related to Combating Payments Fraud**

In the modern banking system, data is the critical component to combating payments fraud effectively. The collection, use, and analysis of data by both industry participants and regulators is crucial to the development of effective fraud prevention strategies, as well as day-to-day fraud monitoring and detection operations throughout the financial services industry. As such, the seamless and transparent movement of data throughout the financial services industry is crucial to combatting payments fraud effectively. Further, the Joint Agencies should engage in analysis of any data they receive regarding payments fraud and convey that information back to industry participants to the extent permissible by law.

Existing programs, such as the Financial Crimes Enforcement Network's (FinCEN) 314(b) program offer an important framework that can be easily applied to the payments fraud issue in a manner that would meet some of the needs for seamless and transparent data movements throughout the financial services industry. Under Section 314(b) of the USA PATRIOT Act, financial institutions—which covers banks, money service businesses, and many other nonbank financial services companies such as casinos and futures commission merchants—may voluntarily share information with one another to identify and report potential money laundering or terrorist financing activities.[5] As part of the 314(b) program, participants are granted safe harbor protections from liability in an effort "to better identify and report activities that may involve money laundering or terrorist activities."[6]

Importantly, while FinCEN's 314(b) program provides a mechanism for data sharing and necessary liability protections to program participants, it does not currently provide industry participants with an effective feedback loop or analysis of the data compiled in the program. As noted above, it is important that the Joint Agencies ensure that a positive feedback loop exists between government and industry. In so doing, the Joint Agencies can assist industry participants in developing improved strategies, as well as day-to-day operations to combat payments fraud. Therefore, AFC recommends that the Joint Agencies

1. pursue a program that will allow industry participants the ability to easily provide data on potential payments fraud activities;
2. operate in a coordinated manner to analyze the information provided; and
3. provide that analysis to industry participants in a manner that will allow these participants the ability to use this information in order to improve their payments fraud strategies and day-to-day operations.

---

[5] 31 CFR § 103.100.
[6] U.S. Department of the Treasury, Financial Crimes Enforcement Network, "Section 314(b) Fact Sheet," Dec. 1, 2020, *available at* https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf.

II. **Recommends that the Joint Agencies Issue an Interagency Policy Statement Affirming That Their Regulations Preempt State Data Privacy Laws that Do Not Exempt Entities or Data Used for Fraud Detection and Prevention Purposes**

As noted above. information sharing and transparent data movement throughout the financial services ecosystem is crucial to combatting payments fraud effectively. Particularly, as consumers increasingly engage directly with fintech companies that partner with innovative banks, ensuring the flow of data between these entities for fraud purposes remains paramount. AFC recognizes the importance of having robust consumer protections regarding the movement, storage, and use of data by industry participants. However, as data issues have become more prominent in federal and state policy conversations, AFC has seen an increase in legislation that impinges upon financial institutions' abilities to leverage consumer data to combat payments fraud.

Under the Gramm-Leech-Bliley Act (GLBA), innovative banks and fintech companies have been able to develop a robust and transparent flow of data to monitor and detect potentially fraudulent activities in payments. While historically, states have exempted both the entities and data covered under GLBA from their data privacy legislation, unfortunately, we have seen these provisions removed from more recent data privacy legislation. Without these specific exemptions for GLBA entities and the data they hold, innovative banks and fintech companies would be subjected to the data deletion and notice requirements in the state laws, including for data used in fraud detection and monitoring activities.

As a result of these state laws, industry participants seeking to comply with prudent risk management practices may find it impossible to comply properly with both existing federal laws, regulations, and Joint Agency rules as well as the new state data requirements. At the very least, these industry participants would face significant obstacles to carrying out federal requirements in the face of these state data requirements. Additionally, this legal uncertainty regarding fraud monitoring and detection practices could significantly interfere with a bank's ability to exercise its powers and to offer its products and services within those states. Further, nefarious actors could use data notice and deletion requirements imposed on innovative banks and their fintech partners to circumvent fraud monitoring and detection processes, increasing risks to consumers.

Given the negative impact that ill-conceived state data privacy legislation and regulation could have on both federal- and state-chartered banks, as well as the issues that would arise from conflicting federal and state requirements, it is imperative that the Joint Agencies invoke their ability to preempt state laws that interfere with a bank's ability to exercise its powers. Specifically, to ensure that both innovative federal- and state-chartered banks, as well as their fintech partners are able to continue conducting crucial fraud detection and monitoring practices, AFC recommends that the Joint Agencies issue an interagency policy statement affirming that their regulations preempt state data privacy laws that do not exempt entities and data covered under GLBA based on the importance of fraud detection and prevention efforts, as well as the data that underpin those efforts, in allowing innovative banks' to exercise their powers under federal banking laws.

III.   **AFC Recommends that The Joint Agencies Incentivize the Use of Innovative Tools to Combat Payments Fraud**

Development of an effective approach to combating payments fraud also requires the Joint Agencies to incentivize the use of technology both by industry participants and the Joint Agencies to root out payments fraud. While AFC recognizes that the human element often presents the greatest challenge when combatting payments fraud, the use of technology tools by both industry participants and regulators—referred to as regtech and suptech respectively— presents an important opportunity to combat payments fraud more effectively. As noted above, for many years, financial institutions have invested in and deployed various regtech tools to combat payments fraud by improving their fraud monitoring and detection processes. Specifically, as payments movements have moved to real-time, so too have fraud monitoring and detection activities.

Using advanced analytics and AI tools, consumer-facing fintech companies can easily identify when consumers may be acting in an abnormal manner that could denote fraudulent activity. Consumers, and their routine engagement with their mobile devices and fintech applications provide a significant amount of data that is exceptionally useful in the fight against payments fraud. Through the use of behavioral analytics tools, industry participants can analyze micro-interactions, such as keystrokes, pauses, and clicks, to understand and measure users' general habits. Further, these tools can quickly determine when micro-interactions with a fintech application do not match the consumer's general habits and flag this interaction for further scrutiny for potential bot activity. In so doing, the behavioral analytics tool can effectively detect potential fraudulent activity and alert the proper individuals and operations about the activity to prevent any fraudulent activity from progressing.

Broader adoption of advanced analytics and AI tools throughout the financial services ecosystem would dramatically improve payments fraud detection and prevention efforts. All of the Joint Agencies have recognized the importance of encouraging responsible innovation and pursuing opportunities to modernize the financial services ecosystem.[7] Further, in virtue of the RFI, as well as other strategic organizational documents, the Joint Agencies have prioritized combatting illicit activities, including payments fraud, in the financial services industry.[8] Taken together, it is clear that the Joint Agencies principally recognize the importance of leveraging responsible innovations as a means to combatting payments fraud.

However, to accomplish this goal, the Joint Agencies must ensure that they have the proper programmatic and regulatory frameworks in place, as discussed above, but also ensure that their examination teams are properly equipped to understand and encourage the use of responsible innovations to combat payments fraud. To that end, AFC believes it is important for the Joint Agencies develop examination curricula and training opportunities that would allow examiners the ability to directly engage with relevant innovations prior to examinations. In practice,

---

[7] See, Board of Governors of the Federal Reserve System, *Strategic Plan, 2024–27* (Washington, DC: Board of Governors of the Federal Reserve System, 2023), *available at* https://www.federalreserve.gov/publications/files/2024-2027-gpra-strategic-plan.pdf; Federal Deposit Insurance Corporation, *2025 Annual Performance Plan and 2024 Annual Performance Report* (Washington, D.C.: Federal Deposit Insurance Corporation, 2025), *available at* https://www.fdic.gov/strategic-plans/2025-annual-performance-plan-and-2024-annual-performance-report; and U.S. Department of the Treasury, *OCC Fiscal Year 2026 Congressional Budget Justification* (Washington, D.C.: U.S. Department of the Treasury, 2025), *available at* https://home.treasury.gov/system/files/266/20.-OCC-FY-2026-CJ.pdf.
[8] Ibid.

concerted efforts to demonstrate innovative technologies to examiners could improve their understanding of the available tools for combatting payments fraud and, in turn, help them assess industry participants' efforts to combat payments fraud more effectively.

*   *   *

AFC appreciates the opportunity to comment the Joint Agencies' Request for Information on Potential Actions to Address Payments Fraud. We welcome continued engagement with the Joint Agencies on this matter and thank you for your consideration of our views.

Sincerely,

Ian P. Moloney
SVP, Head of Policy and Regulatory Affairs
American Fintech Council