MAG
MERCHANT ADVISORY GROUP®
4248 Park Glen Road
Minneapolis, MN 55416
(952) 928-4648

September 18, 2025

Chief Counsel's Office
Office of the Comptroller of the Currency
Attention: Comment Processing
400 7th Street SW Suite 3E-218
Washington, DC 20219
Via www.regulations.gov
OCC: 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
Via https://www.federalreserve.gov/apps/proposals/
Federal Reserve: Docket No. OP-1866

Jennifer M. Jones, Deputy Executive Secretary
Federal Deposit Insurance Corporation
Attention: Comments—RIN 3064-ZA49
550 17th Street NW, Washington, DC 20429
Via https://www.fdic.gov/resources/regulations/federal-register-publications/
FDIC: RIN 3064-ZA49

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

Dear Sir or Madam:

The Merchant Advisory Group (MAG) respectfully submits these comments in response to the Request for Information on Potential Actions to Address Payments Fraud issued by the Office of the Comptroller of the Currency (OCC), Treasury; the Board of Governors of the Federal Reserve System (Board); and the Federal Deposit Insurance Corporation (FDIC) (collectively, the Agencies).

The MAG appreciates the opportunity to comment on this important issue. U.S. merchants are the first line of defense in combating payments fraud, but all too often lack information that is critical to achieve this goal. The Agencies can engage and support merchants by enhancing collaboration, education, regulation, and the tools available to financial institutions. These measures will maximize the information available to all stakeholders

MAG
MERCHANT ADVISORY GROUP®
4248 Park Glen Road
Minneapolis, MN 55416
(952) 928-4648

seeking to prevent fraud, creating a more secure payments ecosystem that benefits all parties involved.

I. Background

About the MAG

The Merchant Advisory Group (MAG) is a global organization dedicated to driving positive change and innovation in the payments industry through merchant collaboration, education, and advocacy. Representing over 175 of the world's leading merchants across many industries, including airlines, retail, restaurants, insurance, amusement parks, grocery, and software, the MAG facilitates strategic engagement across North America, Europe, and Asia.

Like card payments, noncard payments, including check, wire, ACH, and instant payments, pose significant fraud risks, increasing merchants' operational costs and undermining consumer trust. Noncard payments encompass a wide variety of payment methods with differing levels of fraud risk and adoption by U.S. consumers:

- *Checks.* Even though checks are an increasingly rare form of payment, U.S. merchants must devote disproportionate resources to detecting and preventing check fraud.[1] Check fraud tends to be more sophisticated, and therefore harder to detect, than other forms of payment fraud. As a result, check fraud remains one of the most persistent and costly forms of fraud in the payments sector.[2]

- *Instant Payments.* In contrast to checks, instant payments offer an innovative, relatively efficient method of payment that has seen comparatively little fraud.[3] Consumers are adopting this form of payment in increasing numbers.[4] As these payment methods begin to proliferate, they have the potential to facilitate faster, innovative payment approaches that may replace expensive, fraud-prone, and slower card-based forms of payment. As

[1] National Payment Volumes, Detailed Data, DFIPS (CY 2021), Board of Governors of the Federal Reserve System (March 2025) (the number of check payments declined from 13.6 billion in 2018 to 11.1 billion in 2021); The Federal Reserve Financial Services, Key Findings From the Annual Federal Reserve Financial Services (FRFS) Financial Institution Risk Officer Survey (2024), at 4 (check fraud attempts grew by 10% between 2023-2024).

[2] The Federal Reserve Financial Services, Key Findings From the Annual Federal Reserve Financial Services (FRFS) Financial Institution Risk Officer Survey (2024), at 4-5.

[3] *Id.* at 4.

[4] Tom Groenfeldt, Real-Time Payments Are Soaring In The U.S., Forbes (Jul. 17, 2025).

this form of payment continues to gain traction among consumers, strategies to prevent fraud must continue to evolve.

- *ACH and Wire Payments.* The MAG's member merchants typically do not accept ACH or wire payments at the point of sale. However, these payment forms have the potential to serve as secure and efficient forms of payment. The MAG supports efforts to ensure the security of ACH and wire payments as a way to foster continued competition and innovation in retail payments.

Most retail transaction payments today are made by credit or debit card. The card-based payment sector is marked by a persistent lack of competition that has resulted in higher prices and lower quality, including bringing higher rates of payment fraud to the U.S. than in other countries.[5] It is imperative that measures to combat fraudulent noncard payments not drive consumers to use even more costly and fraud-prone card-based payment methods. Accordingly, the recommendations below include measures to ensure a secure and competitive payments ecosystem.

II. External Collaboration

A. Increasing Collaboration with Merchants (Question 1)

Merchants are often the first to deal with the repercussions of fraud and thus have valuable insights into potential solutions. To stay abreast of continually evolving fraud techniques, the Agencies should convene regular roundtables for law enforcement, security experts, financial institutions, merchants, and other stakeholders to discuss emerging fraud trends and prevention strategies. These roundtables can provide a forum for merchants to identify pain points and gaps in resources, while learning from law enforcement agencies about the latest recommended prevention strategies.

Currently, merchants have no definitive source of information regarding fraudulent accounts. Financial institutions are able to share this information among themselves and with certain designated entities under the Safe Harbor Provisions of PATRIOT Act Section 314(b), but merchants are currently ineligible to participate, impeding efforts to detect fraud before a payment is accepted.[6] The Agencies should evaluate ways to grant merchants access to data shared pursuant to Section 314(b) without compromising privacy and security.

[5] *See* Nilson Report Issue No. 1254 (Dec. 2023) at 6 ("The US accounted for 25.21% of global card volume in 2022 but 40.69% of worldwide fraud losses.").
[6] FinCEN, Section 314(b) Fact Sheet, at 2-3.

MAG
MERCHANT ADVISORY GROUP®
4248 Park Glen Road
Minneapolis, MN 55416
(952) 928-4648

The MAG also urges the Agencies to collaborate with merchant and consumer stakeholder groups to develop consumer education programming. Scams and account takeovers targeting consumers are among the most common forms of payment fraud.[7] Focusing educational efforts on consumers, as the most frequent targets of these criminal schemes, is an efficient and effective way to mitigate fraud.

The information-sharing measures discussed above will help prevent fraud and yield benefits for all stakeholders. Although U.S. merchants absorb the costs of fraud, they increasingly lack access to the very information that can enable them to detect and prevent it. The introduction of tokenized account numbers (TANs) illustrates this trend. Because merchants typically evaluate payment risk by payment account and routing number, banks' use of TANs hampers merchants' ability to evaluate fraud risk. As banks apply TANs to more payment types, merchants have less ability to identify possible fraud. Increased collaboration and information-sharing is critical to reverse this dynamic.

B. Types of Collaboration (Question 2)

Accredited standards organizations play a vital role in developing a sound approach to payments security, including noncard payments.[8] These organizations are most effective when they include voices from multiple stakeholders, to achieve collaborative solutions to common problems. The Agencies can support efforts to prevent payment fraud by participating in independent and open standard-setting processes for the development and maintenance of payment security standards. The MAG recommends that the Agencies prioritize collaboration with standards organizations that include merchants as voting members. Merchant participation ensures that standards are not overly burdensome to implement, avoiding a scenario where security practices impose undue costs.

The MAG also recommends that the Agencies collaborate with each other and other government regulators who regulate the financial services industry to undertake transparent rulemaking processes regarding payments security. It is imperative that emerging forms of payment, such as instant payments, are secure and efficient options for consumers in order to drive adoption.

[7] The Federal Reserve Financial Services, Key Findings From the Annual Federal Reserve Financial Services (FRFS) Financial Institution Risk Officer Survey (2024), at 8.

[8] *See, e.g.*, Accredited Standards Committee X9, X9 Creates New Open Forum Focused on Reducing Check Fraud (April 2, 2025) (standard-setting body's open forum focused on reducing check fraud).

MAG
MERCHANT ADVISORY GROUP®
4248 Park Glen Road
Minneapolis, MN 55416
(952) 928-4648

C. Other Organizations Beyond Financial Institutions (Question 3)

The MAG encourages the Agencies to engage with merchant and consumer stakeholders regarding effective measures to detect, prevent, and mitigate payments fraud. These voices are critical to ensure that payment security measures are sound, efficient, and up to date.

D. Federal and State Agency Collaboration to Mitigate Fraud (Question 4)

The MAG strongly advocates for enhanced collaboration between federal and state agencies, law enforcement, and industry stakeholders to combat payments fraud. Increased dialogue and information sharing can help identify emerging trends and develop proactive measures to prevent fraud. Merchants, as key stakeholders, should be actively involved in these discussions to provide insights based on their experiences with payments fraud and related challenges. The Faster Payments Council, launched by the Federal Reserve, is one such industry-led organization addressing faster, cheaper, and more secure forms of payment.

The Agencies should also consider leveraging the expertise of the United States Secret Service, which investigates financial institution fraud.[9] The Secret Service may have useful data about current fraud risks, and best practices to identify, prevent, and mitigate these risks.

The MAG also recommends that State agencies consider measures to securely share RealID numbers with merchants. This would allow merchants to efficiently verify the identity of individuals presenting checks for payment.

III. Consumer, Business, and Industry Education

A. Payments Fraud Education and Audiences (Questions 5-7)

Payment fraud schemes target consumers and small businesses, in particular. The MAG suggests that the Agencies conduct nationwide awareness campaigns targeting these groups.

Effective education should also incorporate the best practices adopted by large merchants to combat payment fraud. Larger merchants have developed innovative methods over the years to stay ahead of evolving fraud schemes. MAG encourages the Agencies to research these best practices as they examine fraud and make recommendations to smaller organizations.

[9] *See* United States Secret Service, Financial Investigations.

MAG
MERCHANT ADVISORY GROUP®
4248 Park Glen Road
Minneapolis, MN 55416
(952) 928-4648

Finally, the MAG urges that the Agencies take steps to target the operations of regional fraud networks. Law enforcement agencies and financial institutions are best placed to provide insight on detecting and disrupting the operations of these networks.

B. Current Effective Resources (Question 8)

From the merchant perspective, some of the most effective resources available online regarding payments fraud are those provided by membership organizations such as the Association of Financial Professionals ("AFP") and Institute of Commercial Payments ("ICP"). The MAG understands that these resources may not be available to nonmembers, such as small merchants, that would benefit from them. The Agencies can fill this access gap by incorporating the teachings of these resources into their own online resources and into future awareness and education campaigns targeted toward small businesses.

IV. Regulation and Supervision

A. Potential Additional Regulatory or Supervisory Actions (Question 9)

The largest contributor to check fraud is the mail system. Fraudsters target U.S. Postal Service facilities and employees to obtain mailed checks, which they then fraudulently alter and deposit.[10] Accordingly, improved security measures at U.S. Postal Service sites are critical. The MAG recommends that the Agencies work with the U.S. Postal Service and Postal Inspection Service to consider regulatory and supervisory efforts to reduce check fraud.

The MAG also recommends that the Agencies promulgate regulations regarding check stock and printing that could make paper checks more difficult to alter or counterfeit. This will mitigate the burden on merchants, who currently bear the cost of detecting fraudulent checks.

As mobile banking continues to grow, more robust safeguards are needed to prevent duplicate presentment of checks. In this scenario, a fraudster deposits a check via mobile device and proceeds to cash the same check in-store. Mobile banking regulations should include measures to protect merchants from this common scheme. Such regulations could prescribe preventative steps for banks, such as requiring customers to write VOID clearly on the face of the check before honoring the deposit. If banks refuse to implement these preventative measures, they should bear the liability for any fraud that results.

[10] FBI & USPIS, Mail Theft-Related Check Fraud is on the Rise (January 27, 2025).

MAG
MERCHANT ADVISORY GROUP®
4248 Park Glen Road
Minneapolis, MN 55416
(952) 928-4648

Finally, the MAG recommends that the Agencies preserve the ability for a merchant cashing a check presented for payment to access the payor's bank account via API in order to confirm routing number, account number, and sufficiency of the account balance.

B. Improving Existing Supervisory Guidance (Question 10)

In order to stay ahead of increasingly sophisticated fraudsters, it is essential that fraud data be shared among law enforcement agencies and, ideally, with merchants and other stakeholders. The MAG urges the Agencies to streamline collection and aggregation of data, leveraging the success of existing payment fraud resources.

The MAG also recommends that the Board undertake comprehensive data collection regarding fraud across all forms of payment, including card and noncard tender forms, and disseminate this data regularly. The Reserve Banks' Depository and Financial Institutions Payments Survey (DFIPS) is one such example of a potential vehicle for this data. This triennial survey of U.S. financial institutions to collect data on noncash payments includes the number and value of those payments, but it does not capture the frequency of fraud using those payment forms.[11] The Survey should be expanded to incorporate aggregate fraud statistics for all forms of payment. This would bring the United States in line with other major economies where such data is systematically collected and reported.[12]

V. Reserve Banks' Operator Tools and Services

A. Enhance Existing Risk Management Tools (Question 21)

The MAG appreciates the Reserve Banks' existing risk management tools and services. In particular, positive pay and positive payee verification tools are paramount in fighting check fraud. Currently, these tools are optional for use by participating financial institutions. The MAG recommends that the Reserve Banks require that all financial institutions use these tools for fraud detection, prevention, and mitigation.

[11] Claire Greene, *Payments Study: Gathering Data from Thousands of Depository Institutions*, https://www.atlantafed.org/blogs/take-on-payments/2025/08/18/payments-study-gathering-data-from-thousands-of-depository-institutions (Aug. 18, 2025); National Payment Volumes, Detailed Data, DFIPS (CY 2021), Board of Governors of the Federal Reserve System (March 2025).

[12] *See* Richard J. Sullivan, *The Benefits of Collecting and Reporting Payment Fraud Statistics for the United States*, Federal Reserve Bank of Kansas City, Payments System Research Briefing (Oct. 2009) at 3.

MAG
MERCHANT ADVISORY GROUP®
4248 Park Glen Road
Minneapolis, MN 55416
(952) 928-4648

B. Expanding Available Risk Management Tools (Question 22)

The Reserve Banks should also consider offering machine learning and artificial intelligence tools to assist financial institutions and merchant businesses in detecting fraudulent activity. Smaller merchants typically lack access to state-of-the-art fraud detection technologies, leaving them more vulnerable to fraudulent schemes. By offering these tools, the Reserve Banks can ensure these small merchants have access to timely, accurate data and ongoing support in their fraud prevention efforts, enabling them to lower prices and improve services for U.S. consumers.

VI. Responses to General Questions

A. Credit Card Payment Fraud Impacts Merchants (Question 23)

Merchant losses from credit and debit card fraud far outpace losses from noncard payments fraud. Payment card fraud remains a persistent problem due to the late introduction of EMV chip and contactless technology by the two dominant card networks, Visa and Mastercard.[13] The persistent lack of competition in the payment card industry has caused U.S. merchants to pay some of the highest costs of card acceptance in the world.[14] In addition to absorbing billions in losses associated with chargebacks, merchants have been forced to expend resources to protect against increasingly complex fraud tactics.[15] The continued prevalence of credit card fraud magnifies the importance of preserving the innovative potential of noncard forms of payment.

VII. Conclusion

The MAG and its members are committed to fostering a secure and efficient payments ecosystem that benefits both merchants and consumers. Noncard payments fraud, though a subset of overall payment fraud, leads to losses for merchants and increased prices for consumers. These costs can be mitigated through expanded access to fraud data, targeted regulations, and continued engagement of merchants and consumers in fraud prevention efforts.

---

[13] *See* Nilson Report Issue No. 1254 (Dec. 2023) at 6 ("The US accounted for 25.21% of global card volume in 2022 but 40.69% of worldwide fraud losses.").

[14] CMSPI, *Back to Basics: Card Network Models and Global Card Costs* (May 29, 2025) (citing global average credit card and debit card fees, with U.S. fees among the highest).

[15] Monica Eaton, Despite New Safeguards, Chargebacks are Rising, Digital Payments (Aug. 1, 2025).

MAG
MERCHANT ADVISORY GROUP®
4248 Park Glen Road
Minneapolis, MN 55416
(952) 928-4648

We appreciate the Agencies' consideration of the merchant perspective and welcome the opportunity to engage further in this process to improve security of noncard payments.

Respectfully,

[redacted]

John Drechny
CEO
Merchant Advisory Group

[redacted]