September 18, 2025

Via www.regulations.gov

Office of the Comptroller of the Currency
400 7th Street, S.W.
Washington, D.C. 20219

Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, N.W.
Washington, D.C. 20551

Federal Deposit Insurance Corporation
550 17th Street, N.W.
Washington, D.C. 20429

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

Ladies and Gentlemen:

Mastercard International Incorporated ("Mastercard") submits this comment letter to the Office of the Comptroller of the Currency ("OCC"), the Board of Governors of the Federal Reserve System ("Board") and the Federal Deposit Insurance Corporation ("FDIC" and, together with the OCC and the Board, the "Agencies") in response to the Request for Information on Potential Actions to Address Payments Fraud (the "Request").[1] Mastercard appreciates the opportunity to provide comments on this important matter.

Background on Mastercard

Mastercard is a technology company in the global payments industry. Mastercard operates a multi-rail payments network that provides choice and flexibility for consumers, merchants and our customers. Mastercard does not issue payment cards of any type nor does it contract with merchants to accept those cards. In the Mastercard network, those functions are performed in the United States by banks and credit unions. Mastercard refers to the financial institutions that issue payment cards bearing the Mastercard brands to cardholders as "issuers." Mastercard refers to the financial institutions that enter into contracts with merchants to accept Mastercard-branded payment cards as "acquirers."

[1] 90 *Fed. Reg.* 26,293 (June 20, 2025).

When a cardholder presents a Mastercard-branded payment card to a merchant to purchase goods or services, the merchant sends an authorization request to its acquirer, the acquirer routes the request to Mastercard, and Mastercard routes the request to the issuer. The issuer either approves or declines the authorization request and routes its decision back to the merchant through the same channels. Mastercard's role in the transaction is to facilitate the payment instructions among the parties to the transaction and to facilitate the clearing and settlement of the payment transaction between the issuer and acquirer.

In addition, as part of our multi-rail strategy to offer consumers and businesses choice in how they transact, Mastercard has expanded payments options to include account-to-account ("A2A") and instant payments capabilities. Today, our technology powers domestic A2A systems in 11 countries across the globe, including real-time and batch payment central infrastructure and overlay services to enhance security and prevent fraud and financial crimes.

In the context of instant payments fraud, Mastercard leverages its expertise from the card payments network and modern technologies such as artificial intelligence ("AI") and behavioral data to identify fraud and scams. This helps banks and network operators protect both senders and receivers in real time. Mastercard's capabilities include end-to-end fraud management platforms with AI scoring, rules management, case management, and business insights modules. These tools enable payment network operators to work collaboratively and effectively with participants to protect customers and build trust.

Comments

The Request sought information on steps that the Agencies can take to mitigate payment fraud with respect to checks, Automated Clearing House, wire and instant payments. Specifically, the Request included five potential areas for improvement and collaboration that could help mitigate payments fraud. Below, we discuss our responses on external collaboration; payments fraud data collection and information sharing; consumer, business and industry education; and Reserve Bank's operator tools and services. We also share information on recent examples of payment fraud in the market.

I. *External Collaboration*

We urge the Agencies to facilitate the establishment of a public-private partnership to help address shared challenges in payment fraud. External collaboration is the first step to fighting fraud. As a founding member of the Aspen Institute Financial Security Program National Taskforce for Fraud and Scam Prevention, we are aligned with the foundational principle that collaboration is essential to ensure data flows across public and private sector ecosystem payments participants to identify, prevent, and minimize cyber attacks and scams.[2]

This public-private partnership should include all stakeholders that have visibility across the kill-chain, including regulators, financial institutions, payment networks, FinTech companies, telecommunications companies, social media companies and law enforcement. Such a

[2] The Task Force develops a unified national strategy to deny transnational crime networks billions of dollars in illicit profits while strengthening U.S. national security and protecting American consumers.

partnership could develop methods for identifying fraud trends, share fraud trends, discuss mitigation strategies, and define common data fields and fraud types. With respect to common data fields specifically, a partnership could develop a standardized fraud taxonomy and a universal scam classification system, which could be based on the Federal Reserve's ScamClassifier model, to improve data consistency. Additionally, a goal of the partnership could be to create consistent metrics and methodologies for tracking scam activities. Individual companies can do much on their own, but partnerships can do much more as a group to combat scams and fraud. Today, there are bilateral agreements and sharing within individual companies, but as an ecosystem we lack a strong collective action piece. Visibility is often limited when it comes to illicit behavior occurring on other companies' systems and in other sectors. With the fraud and scam attack chain covering several sectors, this lack of cross-sector, cross-company insight hinders the ecosystem's ability to identify scams early in their lifecycle and reduce their overall impact. A standardized taxonomy is a key enabler to sharing data.

The Agencies could serve in the role of bringing together participants. An example of successful collaboration is the Financial Stability Board's establishment of the Forum on Cross-Border Payments Data, which was intended to serve as a platform for dialogue, information exchange, and research, helping to identify and address inconsistencies in global data frameworks. The Forum will identify areas of inconsistency in data frameworks related to cross-border payments and facilitate discussion among authorities on how to mitigate frictions while preserving the security of transactions, meeting anti-money laundering and sanctions objectives, preventing fraud and protecting the privacy of individuals.

II. Payments Fraud Data Collection and Information Sharing

We believe that additional data allows for more granular analysis of transactions, helping financial institutions identify unusual patterns or anomalies that might indicate fraud. These data points can be further utilized to understand customer behavior and risk profile over time. In light of the benefits of greater access to data, we support the Agencies taking two steps to increase access to payments fraud data.

First, we encourage the Agencies to facilitate industry development of uniformly-labeled payments data. An example of one joint effort underway with respect to fraud data is the Federal Reserve's FraudClassifier Model, which enables consistent classification of fraud across the industry and participants to discuss data using the same language. There are numerous benefits to the entire payments system from using uniformly-labeled data, including participants having a common understanding, which leads to better future protections; improving interoperability and efficiencies across networks and platforms; and enhancing transparency and traceability.

Second, we ask the Agencies to urge regulators outside of the United States to minimize data localization requirements that could limit or prohibit the transfer of payments fraud data. While many data localization requirements may be intended to support law enforcement and ensure data protection and privacy of consumers, in practice these requirements reduce resilience, expand the attack surface, and restrict the shared ability to defend against transnational cybercriminals by building global models to detect and respond to fraud threats. Cybercriminals take what they have learned in one part of the world and use it to attack another, making defenses that draw only on domestic insights less effective. Reducing the barriers up

front is important given that the transnational nature of cybercrime and fraud complicates law enforcement efforts, and recovering ill-gotten gains across borders is complicated by differing legal frameworks.

III. Consumer, Business and Industry Education

While collaboration between entities and data sharing are crucial factors to mitigating fraud, helping consumers to understand the tell-tale signs of fraud is also critical. With the increasing sophistication of scams, phishing schemes, and unauthorized card use, consumers need to recognize warning signs and understand safe practices. We believe that education on secure payment behaviors can significantly reduce fraud incidents. Card networks already invest in global awareness campaigns, and we ask the Agencies to encourage such efforts from the industry more broadly.

In the context of further consumer education, we also urge the Agencies to explore options to work with ecosystem participants to enable scam detection tools. Beyond scam awareness and digital literacy campaigns, consumers could be further empowered with tools to detect scams prior to manipulation, because once a consumer starts to initiate a payment, it is often too late to protect that consumer from fraud. For instance, in Singapore, tools are being used to not only blocks scam calls and filters suspicious SMS messages, but also enable users to verify potential scams by submitting links, phone numbers, messages, or screenshots for assessment. The technology is available in the United States through several private sector companies and should be considered as an optional feature or service enhancement for participants in payment systems.

IV. Reserve Banks' Operator Tools and Services

As the Request states, the Reserve Banks offer a number of important operational services necessary to facilitating payments and have taken steps to prevent and mitigate payments fraud. We believe the Reserve Banks can enhance their efforts to combat payment frauds by introducing two additional features.

First, the Reserve Banks should implement tools across all of their payment offerings to allow a sender to validate the account of a recipient. In markets where payment system operators have introduced this service, there has been a reduction in fraud losses. For example, the UK has introduced a confirmation-of-payee service across all financial institutions to validate the recipient's name on an account before a transaction is executed. This step, in combination with increased collaboration between financial institutions and the enablement of data sharing, have led to a reduction of fraud in the UK.

Second, we recommend that the Reserve Banks implement network-level/consortium based real-time scoring solutions across all of their payment offerings. This technology works by scanning multiple data points associated with a transaction, providing a risk score – in real time – to the sender's and receiver's bank. Today, we have built a consortium of data permissions, allowing us to see over 90% of all UK A2A payments data, of which 17 banks are protecting their customers with Mastercard's

innovative artificial intelligence AI-powered real-time transaction scoring service, Consumer Fraud Risk ("CFR"). Since its introduction in 2023, CFR played a key role in reducing the number of authorized push payment fraud cases in the UK in 2024 by 20%.

V. *Payments Fraud Generally*

In addition to the other topics in the Request, the Agencies seek information on payments frauds and solutions as well. Mastercard has broad experience with payments in its operation of a payment card network and through its other activities. Because fraudsters do not often limit their behavior to one form of payment, we share our experience with examples of fraud that we have observed for the Agencies' awareness and technology that is helping to reduce fraud.

The development of new technology presents both opportunities and challenges to reducing fraud. Post-pandemic, the increasing adoption of digital payments has significantly expanded the attack surface for fraudsters. New payment systems (some lacking advanced fraud prevention capabilities) contributed to the proliferation of digital fraud and the creation of new risks (e.g., digital wallets and buy-now-pay-later). New technologies, such as generative AI, are making these problems even worse by lowering the barrier of entry for less sophisticated fraudsters to do digital harm. In instant payments specifically, we have seen money stolen through unauthorized fraud or authorized scam and quickly moved on through instant payments transactions and a network of suspect mule accounts. In the absence of an overall network view of this data, individual financial institutions only have a siloed view of the accounts within their portfolio, making it difficult to "follow the funds" to reimburse the victim.

However, despite these hurdles, new technology is allowing the industry to institute new methods to prevent fraud. As discussed above, industry-wide practices are being introduced that allow identity and account verification for recipients of instant payments. In other words, this technology prevents access by fraudulent actors. These enhanced controls, as a supplement to education and awareness efforts, can help mitigate the risk that a consumer will be exposed to malicious activity and thereby reinforce trust across digital platforms.

* * *

If there are any questions regarding our comments, please do not hesitate to contact the undersigned at [redacted] or [redacted]

Sincerely,

[redacted]

Mark R. Klupt
Senior Vice President
Business Development, US