UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Lina M. Khan, Chair**
Rebecca Kelly Slaughter
Alvaro M. Bedoya

In the Matter of	)	
	)	**Docket No. C-4795**
Mastercard Incorporated, a corporation.	)	

COMPLAINT

The Federal Trade Commission, having reason to believe that the Respondent, Mastercard Incorporated ("Mastercard"), a corporation, has violated the provisions of Section 920 of the Electronic Funds Transfer Act ("EFTA"), as amended, 15 U.S.C. § 1693o-2 (colloquially known as the "Durbin Amendment"), and its implementing regulation, Regulation II, 12 C.F.R. § 235 et seq., and therefore of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 41 et seq., and it appearing to the Commission that a proceeding in respect thereof would be in the public interest, hereby issues this Complaint stating its charges as follows:

NATURE OF THE CASE

1. This case is about Mastercard defying rules that Congress and the Federal Reserve Board have adopted to promote competition among companies that process debit card transactions. Mastercard's unlawful conduct frustrates Congress's policy—that merchants who rely on debit cards should be able to choose among processing alternatives—and harms the public interest.

2. Debit cards are used by millions of consumers every day to purchase goods and services of every kind. Over 80% of American adults have at least one debit card; these cards are used to make over $4 trillion in purchases every year. This total slightly exceeds the annual volume of purchases made using credit cards.

3. The volume of debit card purchases made online rather than in stores has grown significantly in recent years, a trend accelerated by the COVID-19 pandemic. Online growth has been particularly rapid for debit cards used in ewallets such as Apple Pay, Google Pay, and Samsung Wallet. Ewallets from these and other providers offer consumers convenience and security benefits and have become increasingly popular.

4. Merchants who accept debit cards, including via ewallets, rely on payment card networks such as Mastercard to process debit card transactions, facilitating the transfer of funds from a consumer's bank account to the merchant's bank account in payment for goods or services. These companies charge fees for each transaction, which are paid directly by merchants and ultimately borne by consumers. Mastercard and Visa are by far the leading payment card networks, and the processing fees networks charge total billions of dollars every year, affecting every purchase made with a debit card.

5. To address concerns about the lack of competition in debit card processing and associated high processing fees, in 2010 Congress prescribed rules for the debit card industry through the Durbin Amendment. Underlying these rules is the principle that merchants must have the opportunity to choose between at least two unaffiliated payment card networks to process debit transactions. It is unlawful for payment card networks like Mastercard to inhibit merchants' ability freely to make this choice.

6. These competition-enhancing rules have led to significant benefits in some areas of debit card processing. But as to the growing field of online ewallet and similar transactions, Mastercard has refused to comply. Instead, it has implemented policies that leave merchants with no choice at all: Mastercard requires merchants to route online ewallet transactions made using Mastercard-branded debit cards to Mastercard for processing—and bear the fees Mastercard charges. Merchants are thus not able to route these transactions to any other payment card network, including networks that may charge lower fees than Mastercard.

7. Absent Mastercard's unlawful conduct, merchants who accept ewallet payments online could have the opportunity to choose among two or more payment card networks to process debit transactions. This freedom to choose among alternative networks would promote the public interest in a competitive debit card ecosystem.

8. Mastercard's conduct violates the Durbin Amendment and Regulation II. If continued or extended to other contexts, these practices would further frustrate the competition-enhancing goals of the law and leave merchants without meaningful choice, to the ultimate detriment of consumers.

RESPONDENT

9. Mastercard is a publicly traded, for-profit company incorporated in Delaware with its principal place of business in Purchase, New York. Mastercard operates a payment card network that enables parties to authorize, clear, and settle transactions using electronic forms of payment, including debit and credit cards. In its 2021 fiscal year, Mastercard earned net revenue of $18.9 billion and net income of $8.7 billion.

JURISDICTION

10. The FTC is vested with authority and responsibility for enforcing, among other things, Section 5 of the FTC Act, 15 U.S.C. § 45, and the Durbin Amendment and Regulation II as to payment card networks and other entities. Violations of the Durbin Amendment and

Regulation II by entities subject to the FTC's authority constitute a violation of the FTC Act, and all of the FTC's functions and powers under the FTC Act are available to the FTC to enforce compliance. 15 U.S.C. § 1693o(c); 12 C.F.R. § 235.9(c).

INDUSTRY BACKGROUND

A. The Debit Card Ecosystem

11. A debit card, as defined in the Durbin Amendment and Regulation II, is any card, or other payment code or device, that is used to debit an account through a payment card network. The processing of debit card transactions involves multiple parties, including: the bank or credit union that issues the card to the cardholder (the "issuer"), the merchant who sells the goods or services, the merchant's bank (called the "acquirer" because it acquires the money to complete the transaction), and the payment card network (the "network") that transmits information between the issuer and the merchant/acquirer.

12. Issuers typically enable for their debit cards (i) one payment card network as a "front-of-card network" (most often Mastercard or Visa), with its brand and logo prominently featured on the front of the card, and (ii) one or more other networks known as "back-of-card networks," often identified on the back of the card. Industry participants also sometimes refer to front-of-card networks as "brand networks," "global networks," or "signature networks" and to back-of-card networks as "competing networks," "alternative networks," "regional networks," "non-affiliated networks," or "PIN networks." Some of this nomenclature was adopted because back-of-card networks developed from regional automated teller machine (ATM) networks and historically processed debit transactions authenticated using a PIN. Much of it is now outdated, though, as back-of-card networks have developed national, non-PIN, and other capabilities.

13. The core function of a payment card network, whether front-of-card or back-of-card, is to transmit information and funds between the merchant/acquirer and issuer. Networks also establish network rules that bind merchants and issuers, and they set the fees paid by merchants to both networks and issuers. Only networks that an issuer has enabled for a debit card can process transactions when a consumer presents that debit card for payment.

14. Whether the transaction is a "card-present" transaction (*e.g.*, with the debit card presented to a merchant in person) or a "card-not-present" transaction (*e.g.*, where the cardholder is not physically present with the merchant, as in ecommerce transactions), a debit card transaction is processed in three main steps: authorization, clearance, and settlement. When the cardholder initiates a transaction with a merchant, the merchant's acquirer sends information about the transaction over the network to the issuer. The issuer decides whether to authorize the transaction and will typically do so when the card is valid, the account has sufficient funds, and the assessed fraud risk is low. Fraud risk can be mitigated by authentication, which is a process designed to establish that the actual cardholder initiated the transaction. Cardholder authentication methods include, but are not limited to, signature, entry of a PIN or passcode on a phone, and biometrics, such as fingerprint or face recognition. Authorization decisions are made nearly instantaneously using automated processes.

15. Once the issuer authorizes the transaction, it must be cleared and settled. Clearance refers to the formal request for payment sent by the merchant to the issuer, again over the network. The final step in the transaction is settlement, which entails the transfer of funds from the issuer to the merchant's acquirer. Clearance and settlement also typically happen in seconds via automated processes.

16. Merchants pay several fees associated with routing debit transactions. Most significant is the "interchange fee," which is paid by merchants (through their acquirers) to issuing banks. Debit interchange fees totaled more than $24 billion in 2019. Also significant is the "network fee," also known as a "network processing fee," paid to networks by both merchants (through their acquirers) and issuing banks. Merchants paid more than $5 billon in network fees for debit transactions in 2019. As the intermediary between merchants and issuers, networks set both interchange fees and network fees. Merchants also pay an "acquirer's fee" for the services of their acquirer. Merchants, and by extension consumers, thus bear most of the cost of authorizing, clearing, and settling debit transactions.

B. The Durbin Amendment

17. The Durbin Amendment, 15 U.S.C. § 1693o-2, was passed in 2010 as part of the Dodd-Frank Wall Street Reform and Consumer Protection Act. The Durbin Amendment instructed the Federal Reserve Board to promulgate implementing regulations, resulting in the publication of Regulation II in July 2011.

18. Congress enacted the Durbin Amendment to prohibit business practices that contributed to high and escalating fees on debit card transactions. Payment card networks and issuers often entered into mutually beneficial agreements requiring merchants to route transactions exclusively to the network on the front of the card, which forced merchants to pay higher fees to both networks and issuers. Networks and issuers also entered into routing priority agreements, which forced merchants to route transactions to certain networks rather than others.

19. As relevant to this Complaint, the Durbin Amendment and Regulation II contain two sets of prohibitions designed to promote merchant and consumer savings associated with processing debit transactions. First, they prohibit network exclusivity by (a) prohibiting a debit card issuer or payment card network from directly or indirectly restricting the number of networks on which a debit transaction can be processed to less than two unaffiliated networks (*e.g.*, Mastercard or Visa can be on the front of the card, and at least one other, unaffiliated network can be on the back of the card), (b) requiring that a debit card issuer enable payment card networks that satisfy certain minimum standards, and (c) prohibiting a payment card network from limiting an issuer's ability to contract with any other network. Second, they prohibit an issuer or payment card network from directly or indirectly inhibiting a merchant's ability to choose which of the networks enabled for the debit card is used to process a given transaction. Congress anticipated these provisions would force networks to compete for merchants' business and thus lower fees. Congress also expected these savings would be passed on to consumers in the form of lower prices.

20. When the Federal Reserve Board first promulgated Regulation II in 2011, many back-of-card networks were capable of processing debit transactions only when authenticated by the cardholder's PIN, that is, where the cardholder is physically present with the merchant at the time of the transaction and enters a PIN on a keypad. This made the back-of-card networks well situated for in-person transactions, but largely unsuited for ecommerce transactions, that is, where the cardholder initiated the debit transaction online or through an application on a mobile device rather than at a physical point of sale.

21. Initially, the requirement of a second, unaffiliated network for all debit cards increased network competition for PIN-authenticated debit transactions, thereby reducing fees charged by networks to merchants. But in contrast, the requirement initially did little to provide merchants with a choice of networks to which to route ecommerce transactions. While the Federal Reserve Board recognized this reality at the time, it acknowledged that back-of-card networks were already in the process of developing the capability to process a broader category of transactions, including ecommerce transactions.

22. Since 2011, many back-of-card networks have developed the predicted capability to process ecommerce debit transactions. By 2019, nearly all back-of-card networks were processing ecommerce debit transactions.

23. Ecommerce debit transactions have come to represent an increasingly important share of the debit landscape. Analyses by the Federal Reserve Board report a marked increase in the volume of ecommerce transactions since 2012, and the shift from in-person to ecommerce transactions accelerated during the COVID-19 pandemic.

C. Tokenization and Ewallets

24. The growth of ecommerce has brought with it a proliferation of digital payment methods, including payment tokens. A debit card can be "tokenized," which refers to replacing the cardholder's primary account number ("PAN") with a different number to protect the PAN during certain stages of a debit transaction. This stand-in number is known as a "token," and the entity that creates the token is referred to as the Token Service Provider ("TSP"). Tokens are stored in lieu of PANs in ewallets such as Apple Pay, Google Pay, and Samsung Wallet. Tokens can also be used in other ecommerce transactions. The token serves as a substitute credential for the PAN to provide additional protection for a cardholder's account number. If the token is stolen, the cardholder's PAN is not compromised. Crucially, issuers have visibility into whether a transaction is tokenized, which gives the issuer greater confidence a transaction is secure and therefore makes the issuer more likely to approve the transaction.

25. TSPs not only create and distribute tokens, but also maintain a "token vault" in which the PAN corresponding to each token is stored. For additional security, TSPs also use cryptograms—a unique number generated for every tokenized transaction based on information about the transaction—to verify whether the token used in a transaction came from a known device associated with the cardholder (*e.g.*, a phone or smart device belonging to the cardholder).

26. Mastercard operates as a TSP for Mastercard-branded debit cards through Mastercard Digital Enablement Service ("MDES").

27. An ewallet—also known as a digital wallet—is a software application ("app") that can store on a mobile phone or other device digital copies of existing debit, credit, and prepaid cards. Popular ewallets include Apple Pay, Google Pay, and Samsung Wallet. Ewallets can be used in-store at a physical terminal, which Mastercard and other payment card networks treat as card-present transactions—while a plastic debit card is not presented, the mobile phone or other mobile device containing the ewallet and tokenized debit card is physically present with the cardholder at the merchant. Ewallets can also be used in ecommerce, including online purchases and "in-app" purchases made within software applications, which Mastercard and other networks treat as card-not-present transactions.

28. When a cardholder loads a Mastercard-branded debit card into an ewallet, Mastercard's rules require use of a corresponding token. The ewallet sends the debit card's information to the issuer to ensure the card data is authentic, and the issuer then uses a TSP to convert the PAN into a token. Issuers of Mastercard-branded debit cards nearly universally use Mastercard (MDES) as the TSP. Once the TSP generates the token, the issuer sends the token to the ewallet, where it is saved for future use in lieu of the PAN.

29. Ewallet tokens are device-centric, meaning each device carrying a particular debit card in an ewallet app has its own, unique token corresponding to the PAN for that card. While there may be multiple tokens associated with each PAN, depending on the number of devices a debit card has been loaded into, only one token for that debit card is associated with each device. Ewallet tokens can be used repeatedly and can be used to make purchases at any merchant who accepts payments via the relevant ewallet.

30. When a cardholder initiates a debit transaction using an ewallet, the merchant receives only the token, not the PAN. The merchant sends the token to its acquirer. The acquirer can then send the token to a payment card network for processing. For the transaction to proceed, however, the network must be able to "detokenize" the token, which includes converting the token to its associated PAN so that the PAN can be sent to the issuing bank. Mastercard can do this for Mastercard-branded debit transactions, as it is almost always the TSP that maintains the token vault containing the required information. Competing networks, however, do not have access to Mastercard's token vault. To route a Mastercard-branded tokenized transaction to a competing network, a merchant's acquirer or a competing network therefore must ask Mastercard to "detokenize" the token.

31. Because debit cards stored in ewallets must be tokenized under Mastercard's rules, a merchant who accepts payments via ewallets must accept the tokens presented. The merchant also has no influence over which TSP provides the tokens. Rather, this is determined by the issuer and is nearly universally Mastercard for Mastercard-branded debit cards. The merchant is thus dependent on Mastercard's detokenization to process ewallet transactions using Mastercard-branded debit cards.

32. A similar dynamic can play out in other ecommerce contexts. For example, with upcoming changes to internet browsers, consumers making online purchases will be able to automatically populate a merchant's website with a Mastercard-issued token. In this scenario, as with ewallets, a merchant would be presented only with a token, which would need to be detokenized by Mastercard to be processed by competing networks.

MASTERCARD'S UNLAWFUL CONDUCT

A. Mastercard's Token Policy

33. Because of the way that payment tokens are designed and maintained, a merchant cannot route a Mastercard-tokenized transaction over a competing back-of-card network without Mastercard's cooperation. Specifically, a merchant's acquirer or a competing network must request that Mastercard's token service (MDES) detokenize the transaction, including by providing the PAN corresponding to the token.

34. For card-present debit transactions using an ewallet—which occur when a cardholder makes a purchase in-store by opening their mobile phone's ewallet application, with a debit card selected to make a payment, and holding the phone to a merchant's terminal—Mastercard will detokenize so that merchants may route the transactions to competing networks. In this scenario, when a merchant decides to route a transaction to a competing network, that network or a merchant's acquirer will request or "call out" to Mastercard's token vault, which will provide the competing network or the acquirer with the PAN associated with the token, as well as validation of the cryptogram.

35. In contrast, Mastercard will not detokenize for card-not-present (ecommerce) debit transactions, including those using an ewallet. Under Mastercard's policy, there is no process by which a merchant's acquirer or a competing back-of-card network can call out to Mastercard's token vault and obtain the PAN or validated cryptogram associated with an ewallet token used in a card-not-present debit transaction, as it can in a card-present transaction. Thus, when a Mastercard-branded card is used in an ewallet for a card-not-present debit transaction, that transaction must be routed over the Mastercard network. Merchants are thus unable to route transactions to back-of-card networks. Indeed, Mastercard requires, and affirmatively tells merchants it requires, that merchants route card-not-present ewallet transactions using Mastercard-branded debit cards to the Mastercard network.

B. Mastercard's Token Policy Is Designed to Increase Mastercard's Debit Revenue

36. Mastercard's token policy reflects a business decision to protect and increase Mastercard's debit revenue, as opposed to any technical limitation on Mastercard's ability to allow merchant routing choice for card-not-present ewallet transactions.

37. Historically, card-not-present transactions have been a safe source of significant revenue for Mastercard, as back-of-card networks once lacked the technical ability to process these transactions, where PIN entry was uncommon. More recently, however, competing back-

of-card networks have developed the capability to route card-not-present transactions, thereby threatening to encroach on Mastercard's profits.

38. At the same time, card-not-present transactions (which encompass both online and in-app transactions) have become an increasingly important portion of debit transactions—as well as an important source of revenue to Mastercard. Card-not-present transactions constituted 31% and 43% of all debit transactions by number and value, respectively, in 2020, a substantial increase from 23% and 37%, respectively, in 2019. These proportions have consistently increased since 2011, when card-not-present transactions made up only 11% and 21% of debit transactions by number and value, respectively. Moreover, the average value of ecommerce transactions is generally substantially higher than that of card-present transactions.

39. These developments represented a threat to Mastercard's debit card revenue and profitability. Mastercard thus adopted and maintained a policy of not detokenizing card-not-present ewallet debit transactions that merchants might otherwise attempt to route over competing networks. The effect of this policy has been to force card-not-present ewallet transactions made with Mastercard-branded debit cards to Mastercard—one of the two leading debit networks—to the detriment of competing back-of-card networks, merchants, and ultimately consumers.

C. Mastercard's Token Policy Inhibits Merchant Routing Choice in Violation of the Durbin Amendment and Regulation II

40. Mastercard's token policy for card-not-present ewallet transactions inhibits merchants' ability to route debit transactions for processing over any available payment card network in violation of the Durbin Amendment and Regulation II.

41. A token stored in an ewallet in lieu of the PAN is itself a debit card governed by the Durbin Amendment and Regulation II. Under both, a debit card is any card, *or other payment code or device*, issued or approved for use through a payment card network to debit an account. Congress and the Federal Reserve Board thus adopted a functional, rather than form-based, definition of a debit card that includes any mode of initiating a debit payment across merchants. The Federal Reserve Board recently confirmed that Regulation II's provisions apply to "information stored inside an e-wallet on a mobile phone or other device, or any other form of debit card." Ewallet tokens are payment codes stored inside an ewallet and used through a payment card network to debit a cardholder's account.

42. Mastercard's policy does not allow card-not-present transactions using ewallet tokens (*i.e.*, debit cards) to be routed to competing debit networks. A merchant thus has only one option: Mastercard's network. Mastercard's policy thereby inhibits the merchant's ability to direct the routing of card-not-present transactions using ewallet tokens over the available network of its choosing.

VIOLATION ALLEGED

43. The allegations in all of the paragraphs above are re-alleged and incorporated by reference as though fully set forth herein.

44. Mastercard's token policy for card-not-present ewallet transactions violates the Durbin Amendment, 15 U.S.C. § 1693o-2(b), and Regulation II, 12 C.F.R. § 235.7, and therefore the Federal Trade Commission Act, 15 U.S.C. § 41 et seq. Mastercard's token policy inhibits merchants' ability to direct the routing of electronic debit transactions for processing over any payment card network that may process such transactions, in violation of 15 U.S.C. § 1693o-2(b)(1)(B) and 12 C.F.R. § 235.7(b). Such acts and practices, or the effects thereof, are continuing and will likely continue or recur in the absence of appropriate relief.

WHEREFORE, THE PREMISES CONSIDERED, the Federal Trade Commission on this thirtieth day of May, 2023, issues its Complaint against Respondent.

By the Commission.

April J. Tabor
Secretary

SEAL