UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

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

In the Matter of	)	
	)	**Docket No.**
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 t(r)3 0 (a)-4 (i)g5 (er)-1 tCtt (a)4 (a)4.e ontully exceeds the annual

de online rather than in stores has grown
COVID-19 pandemic. Online growth has
such as Apple Pay, Google Pay, and

4. Merchants who accept debit cards, including via ewallets, rely on payment card networks such as Mastercard to process debit card transactions,

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 n3 0 Tdng388 0 Td(-)T.0.66 0sorktb( )TJ0 T5.34 -

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," (ev)-0.-9 0.hoo 22

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 of Mastercard (r)3 ((s)-1 (ec)-6 (a)4 (r)3 (l)-2 y u(ni)-2 v)-10 (r)3 (s)-1 (a)4
thw let, wheritis(s)-5 (a)90.9 vhruturs i nli the PA

98. wnlrit(,)e-4s(a(m)-6 e (d)-4 (i)-6 (n)-4 g,(
card io ankeallet(a)4 pp h es isow,c
thee(m)-2 endi4 g(b(e)42(he)-2 (uf-
dbnicardas(en)-4
allet tohe(s)-1 (

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, thaanlerchants irsac (d)TJ0 Tc 0 Tw 17.64 9.02(-)Tj0.33 0 Td[(p)-103M8 (nt)TJ11.61 0 Td(

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

38.

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 ___ day of December, 2022, issues its Complaint against Respondent.

By the Commission.

April J. Tabor
Secretary

SEAL