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

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

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 standardSpan ks

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.

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-

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-