Analysis of Agreement Containing Consent Order to Aid Public Comment

***In the Matter of Mastercard Incorporated,* FTC File No. 201-0011**

I. Introduction

The Federal Trade Commission has accepted, subject to final approval, a consent agreement with Mastercard Incorporated ("Mastercard"). Mastercard operates a payment card network over which merchants can route debit transactions. Mastercard also operates as a token service provider that generates payment tokens for Mastercard-branded debit cards, including tokens saved in ewallet applications on mobile devices.

The consent agreement contains a proposed order addressing allegations in the proposed complaint that Mastercard has inhibited merchants' ability to route electronic debit transactions in violation of the Durbin Amendment, 15 U.S.C. § 1693o-2(b)(1)(B), and Regulation II, 12 C.F.R. § 235.7(b), and therefore also in violation of the Federal Trade Commission Act, 15 U.S.C. § 41 et seq.

The proposed order has been placed on the public record for 30 days to receive comments from interested persons. Comments received during this period will become part of the public record. After 30 days, the Commission will again review the consent agreement and the comments received and will decide whether it should withdraw from the consent agreement and take appropriate action or make the proposed order final.

The purpose of this analysis is to facilitate public comment on the proposed order. It is not intended to constitute an official interpretation of the complaint, the consent agreement, or the proposed order, or to modify their terms in any way.

II. The Complaint

This matter involves allegations that Mastercard's policy with respect to payment tokens saved in ewallets illegally inhibited merchants from being able to route electronic debit transactions to competing payment card networks. The Commission's complaint includes the following allegations.

When a consumer presents a debit card to a merchant to make a purchase, the merchant or the merchant's bank (known as the "acquirer") uses a payment card network (the "network") to communicate with the bank or credit union that issued the card (the "issuer"). If the transaction is approved, the network also handles the transfer of funds. The selection of a network to process a transaction is known as "routing."

Debit transactions can be "card-present" (*e.g.*, where the cardholder presents their debit card to a merchant in person) or "card-not-present" (*e.g.*, where the cardholder is not physically present with the merchant, as in ecommerce transactions made online or through an application on a mobile device). The volume of card-not-present ecommerce transactions has grown

significantly in recent years, including for debit cards used in ewallets such as Apple Pay, Google Pay, and Samsung Wallet.

When a cardholder loads a debit card into an ewallet, the debit card is "tokenized," meaning the primary account number ("PAN") printed on the card is replaced with a different number—the "token"—to protect the PAN during certain stages of a debit transaction. The token service provider ("TSP") that generates the token also maintains a "token vault" that stores the PAN corresponding to each token. When a cardholder initiates a debit transaction using an ewallet, the merchant receives only the token, and not the PAN. The merchant sends this token to its acquirer, which sends the token to a network for processing. For the transaction to proceed, the TSP must "detokenize" the token for the network, which includes converting the token to its associated PAN stored in the token vault.

Mastercard's rules require that a Mastercard-branded debit card that is loaded into an ewallet be tokenized. Mastercard is also the TSP for nearly all Mastercard-branded debit cards used in ewallets. When an ewallet transaction using a Mastercard-branded debit card is routed to Mastercard, Mastercard thus can perform the detokenization and process the transaction. Competing payment card 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 the competing network therefore must ask Mastercard to detokenize the token. Merchants are thus dependent on Mastercard's detokenization to route ewallet transactions using Mastercard-branded debit cards to competing networks.

Mastercard's ewallet token policy leverages tokens to protect its card-not-present ecommerce revenue by inhibiting merchants' ability to route such transactions to competing networks. For card-present debit transactions using an ewallet—which occur when a cardholder makes a purchase in-store by holding their mobile phone with an ewallet application to a merchant's terminal—Mastercard will detokenize so that merchants may route the transactions to competing networks. In this scenario, the merchant's acquirer or competing network will "call out" to Mastercard's token vault, which will provide the PAN associated with the token.

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 network can call out to Mastercard's token vault and obtain the PAN 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, and merchants are unable to route transactions to competing networks. Indeed, Mastercard requires, and affirmatively tells merchants that it requires, that merchants route card-not-present ewallet transactions using Mastercard-branded debit cards to the Mastercard network.

III. Legal Analysis

Mastercard's ewallet token policy inhibits merchant routing choice in violation of the Durbin Amendment, 15 U.S.C. § 1693o-2(b)(1)(B), and its implementing regulation, Regulation II, 12 C.F.R. § 235.7(b).

As part of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, Congress amended the Electronic Funds Transfer Act ("EFTA") to add Section 920, colloquially known as the Durbin Amendment.[1] The Durbin Amendment instructed the Federal Reserve Board to promulgate implementing regulations, resulting in the publication of Regulation II in July 2011.[2] The Durbin Amendment and Regulation II were adopted to address concerns about the lack of competition in debit card processing and associated high processing fees—and they embody the principle that merchants must have the opportunity to choose between at least two unaffiliated networks to process debit transactions.

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, (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.[3] 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.[4]

Violations of EFTA provisions, like the Durbin Amendment, are strict liability offenses.[5] Accordingly, a prospective defendant incurs civil liability merely from its violation of the Durbin Amendment—a showing of scienter, actual harm, or anticompetitive effects is not necessary to establish a violation.[6]

---

[1] Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203 1075 (July 21, 2010) (codified at 15 U.S.C. § 1693o-2).
[2] Debit Card Interchange Fees and Routing; Final Rule, 76 Fed. Reg. 43394 (July 20, 2011) (codified at 12 C.F.R. § 235.1 *et seq*.).
[3] 15 U.S.C. § 1693o-2(b)(1)(A); 12 C.F.R. § 235.7(a).
[4] 15 U.S.C. § 1693o-2(b)(1)(B); 12 C.F.R. § 235.7(b).
[5] *See, e.g.*, *Clemmer v. Key Bank Nat'l Ass'n*, 539 F.3d 349, 355 (6th Cir. 2008) (recognizing an EFTA regulation imposes a strict liability standard); *Burns v. First Am. Bank*, 2006 WL 3754820, at *6 (N.D. Ill. Dec. 19, 2006) ("EFTA is a strict liability statute.").
[6] *See Bisbey v. D.C. Nat'l Bank*, 793 F.2d 315, 318-19 (D.C. Cir. 1986) (holding EFTA does not require proof of actual injury); *FTC v. PayDay Fin. LLC*, 989 F. Supp. 2d 799, 811-13 (D.S.D. 2013) (granting summary judgment to the FTC on violations of EFTA and Regulation E after rejecting justifications not explicitly contemplated by the regulation's language); *Cobb v. PayLease LLC*, 34 F. Supp. 3d 976, 984 (D. Minn. 2014) ("[E]ven where a plaintiff did not suffer damages under the plain terms of the Act, civil liability attaches to *all* failures of compliance with respect to *any* provision of the Act.") (internal quotation marks and citation omitted, emphases in original); *Burns*, 2006 WL 3754820, at *6 ("[A]gain, no necessary scienter . . . Nor must a plaintiff seeking statutory damages prove that he suffered actual damages as a result of a defendant's conduct.").

For purposes of the Durbin Amendment and Regulation II, a "debit card" includes more than the physical piece of plastic found in a cardholder's wallet. 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, regardless of whether authorization is based on signature, personal identification number (PIN), or other means, and regardless of whether the issuer holds the account."[7] Ewallet tokens are payment codes stored inside an ewallet and used through a payment card network to debit a cardholder's account; they are thus debit cards governed by the Durbin Amendment and Regulation II.

Mastercard's ewallet token policy does not allow card-not-present debit 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, in violation of the Durbin Amendment and Regulation II.

Even if, for the sake of argument, an ewallet token is characterized not as a debit card but as a means of access to the underlying PAN, Mastercard still unlawfully inhibits merchant routing choice with respect to card-not-present ewallet transactions. Mastercard requires that all Mastercard-branded debit cards loaded into ewallets be tokenized. And, in fact, nearly all such cards are tokenized by Mastercard—via decisions in which merchants have no say. Because Mastercard tokenizes these cards and then withholds detokenization, card-not-present ewallet transactions are not routable to competing networks—these networks are unable to process the transactions without the corresponding PANs. Mastercard thereby inhibits merchant routing choice by employing a technology that compels merchants to route transactions over Mastercard's network.

Additionally, Mastercard's agreements with ewallet providers require those providers to inform merchants that, by accepting card-not-present transactions through ewallets, merchants agree that transactions made with Mastercard-branded debit cards will be routed to Mastercard. Mastercard thereby inhibits merchant routing choice by contract.

IV. Proposed Order

The proposed order seeks to remedy Mastercard's illegal conduct by requiring Mastercard to provide PANs so that merchants may route tokenized transactions using Mastercard-branded debit cards to the available network of their choosing. Under the proposed order, Mastercard must also refrain from interfering with the ability of other persons to serve as TSPs, and it must not take other actions to inhibit merchant routing choice in violation of Regulation II, 12 C.F.R. § 235.7(b).

Section I of the proposed order defines the key terms used in the order.

Section II of the proposed order addresses the core of Mastercard's conduct. Paragraph II.A. requires Mastercard, upon request by an authorized acquirer, authorized network, or other authorized person in receipt of a Mastercard token, to provide the PAN

[7] 12 C.F.R. § 235.2(f)(1) (emphasis added); 15 U.S.C. § 1693o-2(c)(2).

associated with the token for purposes of routing the transaction to any competing network enabled by the issuer. This provision is designed to restore and preserve merchant routing choice so that merchants may accept ewallet tokens without being forced to route all such transactions over Mastercard's network. The order specifically requires that Mastercard provide PANs for ecommerce, card-not-present debit transactions in the ordinary course, including in a manner consistent with the timeliness with which Mastercard provides PANs for card-present transactions and without requiring consideration for making the PANs available.

Paragraph II.B. prevents Mastercard from prohibiting or inhibiting any person's efforts to serve as a TSP or provision payment tokens for Mastercard-branded debit cards. This paragraph prevents Mastercard from taking other actions that would inhibit merchant routing choice in the context of tokenized transactions.

Paragraph II.C. prohibits Mastercard from, directly or indirectly by contract, requirement, condition, penalty, or otherwise, inhibiting the ability of any person that accepts or honors debit cards for payments to choose to route transactions over any network that may process such transactions, in violation of Regulation II, 12 C.F.R. § 235.7(b). This paragraph prevents Mastercard from taking other actions, even outside the context of tokenized transactions, that would inhibit merchant routing choice.

The proposed order also contains provisions designed to ensure Mastercard's compliance with the order. Section III requires Mastercard to provide notice to competing networks, acquirers, and issuers via an ad hoc Mastercard bulletin using language found in the proposed order's Appendix A.

Section IV requires Mastercard to provide prior notice to the Commission before the commercial launch of any new debit product that requires merchants to route debit transactions to Mastercard's network.

Sections V through VII contain provisions regarding compliance reports to be filed by Mastercard, notice of changes in Mastercard, and access to Mastercard documents and personnel.

As stated in Section VIII, the proposed order's purpose is to remedy Mastercard's alleged violation of the Durbin Amendment, EFTA Section 920(b)(1), 15 U.S.C. § 1693o-2(b)(1), as set forth by the Commission in its complaint. Section IX provides that the order will terminate 10 years from the date it is issued. However, if the United States or Commission files a complaint in federal court alleging a violation of the proposed order (and the court does not dismiss the complaint or rule that there was no violation), then the order will terminate 10 years from the date such complaint is filed.