Meeting Between Staff of the Federal Reserve Board and Representatives of PIN Debit Networks, Merchants, Merchant Trade Groups, and Counsel
June 11, 2019

Participants: Clinton Chen, Lacy Douglas, Susan Foley, Mark Manuszak, Emily Massaro, David Mills, Hayden Parsley, and Krzysztof Wozniak (Federal Reserve Board)

Owen Glist and Jeffrey Shinder (Constantine Cannon); David Chiappetta and Kimberly Ford (First Data); Jennifer Hatcher (Food Marketing Institute); Elizabeth Provenzano (Merchant Advisory Group); Robert Yeakel (National Grocers); Stephanie Martz (NRF); David Schneider (Pulse Network); Eric Citron and Austen Jensen (RILA); Daniel Kramer (Shazam); Douglas Kantor (Steptoe & Johnson); Amy Oberhelman (Target); Reed Luhtanen (Walmart)

Summary: Staff of the Federal Reserve Board met with representatives of several PIN debit networks, merchants, and merchant trade groups to discuss their observations pertaining to card-not-present routing of debit card transactions and tokenization in the market. The representatives also discussed the implementation of EMVCo's Secure Remote Commerce specifications.

Attachment

June 3, 2019

TO: [redacted] Federal Trade Commission

FROM: National Retail Federation

RE: **Visa's and Mastercard's Continuing Violations of the Durbin Amendment**

I. EXECUTIVE SUMMARY

During our past meetings, you requested that we summarize in writing the ongoing misconduct by Visa and Mastercard that inhibits merchant choice in violation of the Durbin Amendment and its implementing regulations (Regulation II, 12 C.F.R. Part 235, Debit Card Interchange Fees and Routing). This misconduct may generally be divided into two categories:

Misuse of technology to inhibit merchant choice:

- Manipulating AID selection and mandating prioritization of the Global AID
- Refusing to license non-PIN CVMs to the Common AID
- Prohibiting merchants from requiring a PIN at the point of sale
- Requiring the routing of tokenized in-app and card-on-file transactions to global networks
- Creating a joint "check out" button that blocks other networks

Misuse of market power to inhibit merchant choice:

- Entering into volume agreements that penalize issuers for enabling competing networks' No-CVM and Signature-authentication products
- Charging issuers a Volume Assessment Fee to penalize them for transactions routed over other networks
- Entering into signature debit exclusivity contracts with issuers
- Tying merchant pricing for non-routable transactions to the volume of the merchant's routable transactions

II. VISA'S AND MASTERCARD'S ANTICOMPETITIVE CONDUCT IS AN EFFORT TO QUASH INCREASED COMPETITION FOSTERED BY THE DURBIN AMENDMENT

Understanding how Visa and Mastercard achieved their historical dominance in debit helps explain why they are acting anticompetitively in violation of the Durbin Amendment and its implementing regulations in an effort to protect their debit market share.

The first debit cards were introduced by so-called "regional debit networks," such as PULSE and STAR.[1] These networks were originally built to process ATM transactions but were expanded to also process debit transactions at the point of sale when card-issuing banks realized that allowing the use of ATM cards at the point of sale would significantly reduce their expenses relating to processing checks. Since these debit networks grew out of ATM networks, and since ATMs have always required the increased security of a Personal Identification Number ("PIN") to authenticate the identity of the cardholder, all debit transactions similarly originally required that the cardholder enter a PIN at the point of sale.

Visa and Mastercard -- each of which owned a credit card network -- grew concerned that the increasing volume of debit transactions at the point of sale could potentially erode the volume of credit card transactions. Therefore, they each launched their own debit network. These are referred to as the "global networks," since Visa and Mastercard each have operations outside of the United States. Unlike the competing debit networks that used the increased security of PIN authentication, the global debit networks chose to use their existing infrastructure and supported only signature authentication for their respective networks at the point of sale.

The fees charged to merchants for Visa and Mastercard signature debit transactions were significantly higher than those charged by the competing debit networks for PIN debit transactions. Since a significant portion of these increased fees were paid to the issuing banks in the form of interchange, these banks readily enabled their existing debit cards for either the Visa or Visa or Mastercard signature debit network.[2] However, issuing banks also retained at least one, and often three or four competing debit networks on their cards, since the more secure PIN authentication offered by these networks was necessary to allow ATM access. As such, each debit card was generally enabled for a single global network that authenticated transactions by signature, and one or more competing debit networks that authenticated transactions by PIN.

While issuing banks were enthusiastic about the higher fees charged for Visa and Mastercard debit transactions, Visa and Mastercard realized that the merchants who paid these fees would be

[1] Since these networks originally operated only in certain regions of the country, they are colloquially referred to in the industry as the "regional debit networks." However, since most now operate nationwide, they are referred to as the "competing debit networks" throughout this memorandum, while Visa's and Mastercard's networks are referred to as the "global networks."

[2] To avoid competition between Visa and Mastercard, each network enforced rules prohibiting issuing banks from enabling both global signature networks on a single debit card. While these rules were invalidated when the Durbin Amendment was enacted, *see* 12 C.F.R. § 235.7(a)(3), no issuing bank to this day has enabled both Visa's and Mastercard's signature networks on its cards.

reluctant to accept Visa's and Mastercard's new offerings. Rather than lowering fees to encourage merchant acceptance, Visa and Mastercard instead forced merchants to accept their debit products by tying them to acceptance of their respective dominant credit products. If a merchant wished to continue accepting Visa's and Mastercard's ubiquitous credit products (which, because of the dominance established by Visa and Mastercard in the credit card market, was an economic necessity), it was required to also accept their undesirable and expensive signature debit products. Absent this tying, merchants would have had little incentive to accept Visa and Mastercard debit cards. This anticompetitive practice was only abandoned years later in settlement of a class action antitrust lawsuit, after Visa and Mastercard had already seized a large share of the debit market.

Since the competing debit networks traditionally supported only PIN authentication while Visa and Mastercard supported only signature authentication, the method of authentication used at the point of sale historically dictated the network over which a given transaction could be processed. Whenever a cardholder did not enter a PIN, the merchant had to process the transaction over the single global network for which the card was enabled -- either Visa or Mastercard. This gave Visa a monopoly over non-PIN transactions on Visa-enabled cards, and Mastercard a monopoly over non-PIN transactions on Mastercard-enabled cards.

In an attempt to capture PIN transactions as well, Visa and Mastercard also each acquired a PIN-authenticated debit network -- with Visa purchasing Interlink and Mastercard forming Maestro -- which allowed them to compete with the competing debit networks for PIN-authenticated debit transactions. Meanwhile, Visa and Mastercard each continued to maintain their respective monopolies over non-PIN transactions.

To strengthen their monopolies, Visa and Mastercard took additional steps to inhibit merchant network choice. For example, in concert with their issuing banks, they encouraged cardholders to "skip the PIN to win" and authenticate by signature, which would force the merchant to send the transaction to Visa or Mastercard at a substantially higher cost. Visa and Mastercard each also entered into exclusivity agreements with issuers, paying them significant sums in return for the issuer agreeing to enable debit cards only with networks owned by either Visa or Mastercard. This resulted in a proliferation of Visa/Interlink and Mastercard/Maestro debit cards. When one of those cards was presented for a purchase, the merchant's only choice was to process the transaction over either a Visa-owned network or a Mastercard-owned network, depending on the card. This gave the global networks a monopoly over *all* transactions on these debit cards, forcing the merchant to pay higher fees regardless of the form of authentication used.

Over the years, Visa and Mastercard have repeatedly acted to beat back threats to their respective monopolies and dominant debit market share. The most recent instance of this involves their response to two significant developments. First, the Dodd-Frank Act of 2010 included the Durbin Amendment. On July 20, 2011, the Federal Reserve issued implementing regulations (Regulation II, 12 C.F.R. Part 235, Debit Card Interchange Fees and Routing) which relevantly [1] prohibited exclusivity agreements by requiring that all debit cards be enabled for at least two *unaffiliated* debit networks, [2] prohibited networks from inhibiting an issuer's ability to contract

with competing networks, and [3] prohibited networks and issuers from inhibiting the merchant's ability to process each debit transaction over any of the networks for which the card was enabled. Second, to afford merchants the opportunity to benefit from debit network choice on all transactions as contemplated by the Durbin Amendment, and to facilitate network competition on all transactions, the major competing debit networks began to develop their own signature-authentication and no-CVM technologies[3] that allow them to process transactions even when the cardholder does not enter a PIN.

As a result of those developments, each Visa-enabled card should be enabled for at least one network not affiliated with Visa, and each Mastercard-enabled card for at least one network not affiliated with Mastercard. Moreover, at least in theory, merchants should be able to process transactions over the unaffiliated network even if the cardholder does not enter a PIN, such that one or more of the competing debit networks could now compete for every transaction at the point of sale. However, as described below, to protect their respective monopolies, Visa and Mastercard each responded with actions that inhibit merchant choice in violation of the Durbin Amendment and its implementing regulations, thus precluding the increased competition that the law was intended to foster.

III. VISA AND MASTERCARD MISUSE TECHNOLOGY TO INHIBIT MERCHANT DEBIT ROUTING CHOICE

Virtually every debit card issued in the United States is enabled for Visa or Mastercard.[4] As a result, merchants, card issuers, acquirers, and processors alike are required to adopt technologies that are developed and mandated by the two global networks.

While Visa and Mastercard mandate the adoption of certain technologies through their rules, they use financial coercion to compel the adoption of others. For example, when Visa and Mastercard decided that the United States should adopt EMV chip card technology[5] developed by EMVCo,[6] Visa and Mastercard promulgated rules imposing a "liability shift" upon all issuers and merchants that did not adopt EMV technology. Under that "shift," if certain types of fraud occurred on a transaction involving an issuer and a merchant, only one of which had adopted

[3] "No-CVM" means that the transaction may be processed without a signature, PIN, or any other verification of the cardholder's identity. This allows merchants to minimize the time spent by the cardholder at the point of sale.
[4] A small number of debit cards are instead enabled for the Discover network. For decades, due to other anticompetitive actions of Visa and Mastercard, Discover has been unable to make significant inroads against Visa's or Mastercard's market shares in debit.
[5] Under EMV chip card technology, a computer chip is included on each credit and debit card issued. This makes it more difficult to create a counterfeit card, as that would require creating a duplicate of the chip. However, this technology does not address cardholder authentication as it does not make it any more difficult for an impersonator to use a lost or stolen chip card.
[6] EMVCo LLC is the company that developed EMV chip card technology. "EMV" stands for Europay, Mastercard, and Visa, the three original owners of EMVCo. Europay was acquired by Mastercard in 2002, leaving Visa and Mastercard as the sole owners of EMVCo. In the years that followed, JCB, American Express, China UnionPay, and Discover were admitted as equity owners of EMVCo, but Visa and Mastercard retained their status as "founding members," with special voting rights. No competing debit network has ever been permitted to join the EMVCo consortium.

EMV technology, liability for the transaction would be shifted to the party that had not adopted EMV technology, regardless of fault. With their market dominance, Visa and Mastercard thereby effectively forced the adoption of their EMV chip card technology without technically "mandating" it.[7] In doing this, Visa and Mastercard foreclosed the development and adoption of competing technologies then being developed. Visa and Mastercard have similarly forced the adoption of other technologies they own. After using market power to force adoption of such technologies, Visa and Mastercard have often used those technologies to disadvantage competing networks and inhibit merchant choice, as described below, in violation of the law.

A. Visa and Mastercard Inhibit Merchant Debit Routing Choice by Manipulating AID Selection and Mandating Prioritization of the Global AID

By imposing the EMV liability shift, Visa and Mastercard effectively required merchants to replace their point-of-sale terminals with new terminals capable of reading EMV chip cards and processing EMV transactions, and required issuers to physically embed EMV chips in their respective debit cards. Each EMV chip card contains a computer chip encoded with an "application" that facilitates the transmission of information, and application identifiers ("AIDs") that instruct the application how to process the transaction. Visa owns the technology behind the applications and associated AIDs on all Visa-enabled debit cards, and Mastercard owns the technology behind the applications and AIDs on all Mastercard-enabled debit cards.

Visa and Mastercard originally intended to license to U.S. issuers only one type of AID -- a "Global AID" that supported only transactions carried over their respective networks.[8] This would ensure that all EMV transactions were routed to either Visa or Mastercard, excluding and potentially destroying the competing debit networks. These plans were disrupted by the Durbin Amendment and its implementing regulations, which required EMV technology to also support transactions over these competing debit networks.

Visa and Mastercard decided not to allow the competing debit networks to process transactions over their existing Global AIDs, as they did not want to afford equal footing to the competing networks. Instead, in an effort to appear as if they were complying with the Durbin Amendment and its implementing regulations, each created a separate "Common AID," As a result, each debit card issued in the United States now has two AIDs: (1) a Global AID that routes all transactions solely to the global network enabled on the card (either Visa or Mastercard);[9] and (2) a Common AID capable of routing transactions to any network for which the card has been enabled (including one or more competing debit networks and also including either Visa or

[7] Prior to the introduction of EMV, cardholder information was contained on a magnetic stripe ("mag stripe") on the back of the card. The mag stripe was not proprietary, and it facilitated routing to all networks without any limitations. The shift to EMV by issuers and merchants, required to avoid the EMV liability shift, gave control over these specifications to the global networks.

[8] This is what Visa and Mastercard did in other countries where EMV technology has been implemented. For example, Visa-enabled cards issued in Europe support only Visa transactions.

[9] Visa Rule 4.1.19.55 (which has been renumbered several times over the past few years but never repealed) mandates that all transactions processed over the Global AID must be routed to Visa.

Mastercard). Visa and Mastercard have since used the existence of these two AIDs to suppress competition in various ways.

For example, following implementation of the Durbin Amendment, Visa continued to enforce its Rule 1.5.4.6, which required merchants to allow the cardholder to select the network over which a debit transaction is to be processed, even though the Durbin Amendment and its implementing regulations are clear that routing choice belongs to the merchant. In its technical documentation, Visa provided three methods by which merchants could comply with this rule.[10] Two of these methods involved displaying confusing "cardholder choice" selection screens at the point-of-sale. These screens did not make clear to the cardholder the significance of the choices being provided and were designed by Visa to trick the cardholder into "choosing" Visa, thereby requiring merchants to route the transaction to Visa under Rule 1.5.4.6 and eliminating merchant routing choice.[11]

If merchants did not present one of these Visa-approved confusing and misleading selections to cardholders, the merchant was instead required to program their terminals to select the AID based upon the "priority" encoded on the debit card by the issuer. But Visa's rules require that all issuers prioritize the Global AID (which routes only to Visa) over the Common AID (which supports routing to all networks including Visa). The result is that, if merchants did not display one of Visa's confusing and misleading screens at the point of sale, Visa's rules required that all debit transactions be routed solely to Visa.

In 2016, in response to requests from merchants, competing networks, and consumer advocacy groups, the Federal Reserve and FTC each made inquiries into Visa's rules and technical specifications that were resulting in the terminal screens requiring cardholders to select the AID. The Federal Reserve ultimately issued a Regulation II FAQ on November 2, 2016, specifying that any network rule mandating that a merchant allow the cardholder to select the AID was a violation of 12 C.F.R. § 235.7(b), since the Global AID supported only a single network.[12] Meanwhile, the FTC launched a formal investigation that resulted in Visa repealing Rule 1.5.4.6 and amending its technical specifications. However, despite continuing demands from industry participants, Visa has retained its AID priority rule which requires that the Global AID must be

[10] Visa's technical specifications such as its Transaction Acceptance Device Guide ("TADG") and Acquirer Information Guide ("AIG") purported to identify a fourth method, but that method did not comply with Visa Rule 1.5.4.6, since it did not allow the cardholder to select the network. Kroger discovered this when, having relied on Visa's technical documentation to install terminals using this fourth method, Visa fined it tens of millions of dollars. Visa then informed Kroger that the fines would stop if Kroger routed all non-PIN authenticated transactions to Visa.
[11] The first option approved by Visa was for the merchant's terminal to be programmed to ask the cardholder to choose between "Visa Debit" and "US Debit," with no explanation provided to the cardholder. Visa's rules provided that only if the cardholder selected "US Debit" -- a term that is meaningless to consumers and would therefore rarely be selected -- could the transaction be routed to the Common AID that preserved merchant debit routing choice. The second option approved by Visa required merchants to route all *debit* transactions to Visa whenever the cardholder selected "*credit*" at the point of sale, even though that was not the cardholder's intent in making this selection.
[12] See https://www.federalreserve.gov/paymentsystems/regii-faqs.htm (§ 235.7, Question 4).

prioritized over the Common AID, even though only the latter preserves debit network routing choice for the merchant.

As a result of Visa's technical specifications described above and the standardized EMVCo specifications,[13] there are millions of terminals already installed at merchant locations throughout the United States that select the AID based on priority. And there is nothing *per se* wrong with those terminals. In fact, if the Common AID were prioritized on all debit cards issued in the United States, these terminals would promote competition by routing all debit transactions to the Common AID, thereby enabling merchant network choice on each transaction. This is what was anticipated by the other participants in the payments system when Visa and Mastercard introduced the two AIDs. The problem lies in Visa's and Mastercard's rules requiring issuers to prioritize the Global AID over the Common AID. Solely because of these rules, terminals programmed to automatically select the priority AID instead route all debit transactions to Visa or Mastercard and deprive merchants of all debit routing choice on all debit transactions. Those rules therefore violate 12 C.F.R. § 235.7(b) because they inhibit merchant routing choice.

Visa and Mastercard have taken the position that merchants who have installed priority-based terminals and want routing choice can either reprogram their terminals or purchase new ones.[14] But many merchants (particularly smaller ones) are unaware that their terminals are -- due to Visa's and Mastercard's AID prioritization mandate -- taking away their routing choice in the first place. Merchants should not be required to police the networks' compliance with the Durbin Amendment, nor bear the burden of learning the intricacies of EMV technology and how to avoid the effects of Visa's and Mastercard's AID prioritization rules. More to the point, they certainly should not be required to spend the significant resources required to reprogram their terminals[15] or purchase new terminals to avoid the effects of Visa's and Mastercard's AID-priority rules and preserve their network routing choice. The Federal Reserve has stated that network actions imposing additional costs on a merchant's use of a competing network violate 12 C.F.R. § 235.7(b), because they inhibit merchant routing choice.[16] Visa's and Mastercard's AID prioritization mandate, requiring merchants to incur significant funds to reprogram their

[13] EMVCo's specifications (which are global in nature and not promulgated with the Durbin Amendment in mind) direct that EMV terminals must be programmed to select the AID by: (1) requiring the cardholder to select the AID; or (2) automatically selecting the highest-priority AID. (See EMV Integrated Circuit Card Specifications for Payment Systems Book 4, Version 4.2, § 11.3).

[14] This is similar to the position taken by Visa when its rules and specifications requiring the "Visa Debit" and "US Debit" screens were first questioned by the FTC and Federal Reserve. It is noteworthy that even though those rules and specifications have since been repealed due to the actions of the FTC and Federal Reserve, there remain a significant number of these terminals in use, particularly at smaller merchants' locations. This is no surprise since replacing or reprogramming terminals is an expensive endeavor, assuming the merchant even knows and understands the issues. It is also a testament to how important it is to timely quash the use of technology for anticompetitive means, since it is difficult to replace or repair technology once it has been distributed in the marketplace.

[15] For many merchants, the cost of reprogramming terminals is prohibitively expensive, and often more expensive than purchasing new terminals.

[16] See the Federal Reserve's "Frequently Asked Questions About Regulation II (Debit Card Interchange Fees and Routing)," https://www.federalreserve.gov/paymentsystems/regii-faqs.htm, retrieved on June 3, 2019, § 235.7, Question 2.

terminals or purchase new terminals to preserve their routing choice, squarely falls within the conduct that the Federal Reserve has declared to be a violation of the Durbin Amendment and its implementing regulations.

Visa's and Mastercard's AID prioritization rules also serve to bar issuers from entering into incentive or other agreements with competing debit networks to prioritize the Common AID and thus preserve merchant debit networking routing choice. Were an issuer to enter into such an agreement, the issuer would be fined increasing amounts by Visa or Mastercard for violating their respective AID prioritization rules. These rules therefore separately violate 12 C.F.R. § 235.7(a)(1), which provides that a network may not limit an issuer's ability to contract with any other network.

B. Visa and Mastercard Inhibit Merchant Debit Routing Choice by Refusing to License Non-PIN CVMs to the Common AID

Unlike the previous mag stripe technology which was developed by an open standard-setting body, Visa and Mastercard own the intellectual property behind the Global AID and Common AID that reside on each EMV debit card that is enabled for their respective networks. Since neither network would allow transactions on the Global AID to be processed over the competing debit networks, the Durbin Amendment and its implementing regulations compelled the global networks to license to these networks the ability to process transactions over the Common AID, as EMV debit cards would otherwise not be Durbin-compliant.[17] However, Visa and Mastercard have only licensed the competing debit networks to process PIN and no-CVM transactions over the Common AID. They have refused to license any other CVM, including the signature CVMs now offered by the competing debit networks, or other emerging CVM technologies such as biometrics.

The result of this refusal is that whenever a cardholder verifies a transaction with a non-licensed CVM such as signature or biometrics, the merchant must give up its routing choice and send the transaction to the Global AID (and therefore to Visa or Mastercard) if it wishes to inform the network how the transaction was authenticated. If the merchant instead uses the Common AID necessary to preserve its network routing choice, the merchant and the competing network must falsely represent to the issuer that the transaction was a no-CVM transaction, even though it was authenticated by signature or biometrics. Doing so decreases the issuer's ability to detect fraud and increases the risk that the transaction will be declined and/or that liability will be shifted to

[17] The Federal Reserve was clear in its rulemaking that developers of new technology must accommodate the network exclusivity and dual routing requirements of the Durbin Amendment for every transaction on each debit card, code, or other access device. *See*, 76 Fed. Reg. 43419 (Jul. 20, 2011) ("The Board has considered the comments and has determined that new or emerging access devices are included within the scope of the proposed rule if they are issued or approved for use through a payment card network and otherwise meet the criteria for being a debit card as the term is defined in this rule (e.g., the card, code, or device debits the cardholder's account or a general-use prepaid card."); 12 C.F.R. § 235.2(f) ("Debit card (1) Means 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…").

the merchant. Visa's and Mastercard's refusal to license non-PIN CVMs therefore inhibits merchants from selecting the Common AID -- which is necessary to preserve their network routing choice -- in violation of 12 C.F.R. § 235.7(b).

The adverse effect on merchants resulting from Visa's and Mastercard's refusal to license non-PIN methods of authentication over the Common AID continues to grow, as biometric authentication methods such as Touch ID and facial recognition -- now present on the iPhone and other smart phones -- increase in popularity. This refusal also adversely affects efforts by acquirers and merchants to develop and implement their own authentication methods that would further reduce fraud. None of these technologies was even developed by Visa or Mastercard. For example, Apple developed the Touch ID and facial recognition technologies installed on iPhones to secure payment transactions processed over these devices. By allowing the Global AID to support these technologies, Visa and Mastercard are able to inform the issuer that one of these technologies was used when the transaction is processed over their networks. But by refusing to allow these technologies to be used for transactions processed over the Common AID, Visa and Mastercard are prohibiting the merchant from informing the network or the issuer that one of these technologies developed by Apple was used to authenticate a transaction processed over a competing debit network. The result is that the merchant's routing options are inhibited since, if wants to use these independently-developed technologies, it must route EMV transactions over the Global AID solely to Visa or Mastercard and cannot route the transaction to any competing network. Visa and Mastercard are thereby using their control over EMV technology and the Common AID to force merchants who wish to use these security features, none of which is proprietary to Visa or Mastercard, to forfeit their network routing choice, in violation of 12 C.F.R. § 235.7(b).[18]

Visa's and Mastercard's refusal to license non-PIN CVMs on the Common AID also inhibits issuers' ability to contract with the competing debit networks in violation of 12 C.F.R. § 235.7(a)(3). If an issuer wishes to contract with a competing debit network to accept signature or biometrically-authentication transactions, Visa and Mastercard prohibit the competing network from informing the issuer that the transaction was actually authenticated through one of these mechanisms -- or at all. This significantly denigrates the utility of these authentication methods for the issuer, likely resulting in the issuer not contracting with the competing network to enable them. This not only violates the Durbin Amendment and its implementing regulations by inhibiting issuers' ability to contract with the competing debit network, but also stifles competition by interfering with these networks' ability to roll out these competing features.

C. Visa Inhibits Merchant Debit Routing Choice by Prohibiting Merchants from Requiring a PIN at the Point of Sale

Prior to the Durbin Amendment, and before the competing debit networks developed the ability to process signature transactions, Visa enacted a rule prohibiting merchants from requiring that

[18] Were Visa and Mastercard to license the competing debit networks to process non-PIN forms of authentication over the Common AID, the logistics behind this would be carried out by the acquirer -- and not Visa or Mastercard -- simply by including a data element in the authorization data that is already flowing over the Common AID.

cardholders enter a PIN and requiring merchants to allow cardholders to instead authenticate by an alternative method such as signature. Since Visa was, at that time, the only network that could process signature-authenticated transactions on Visa-enabled debit cards, this rule helped Visa expand its overall market share in debit. If a merchant wished to require that a cardholder enter a PIN so that the merchant could route the transaction to one of the less-expensive competing debit networks while also obtaining the increased security, reduced fraud, and resulting decrease in chargebacks resulting from PIN authentication, the merchant risked being fined by Visa.

While the competing debit networks have since developed features enabling them to process signature and no-CVM transactions, many issuers have not yet enabled these features, primarily due to the actions of Visa and Mastercard described in Sections IV.A-IV.D below. Therefore, all non-PIN transactions on those issuers' cards must still be routed to Visa or Mastercard, preserving Visa's and Mastercard's respective monopolies over non-PIN transactions on these cards.[19] Knowing this, Visa has retained its rule prohibiting merchants from requiring that cardholders enter a PIN, thus allowing the cardholder and not the merchant to select the debit network over which the transaction is carried.[20] Visa has reiterated its intention to continue to enforce this rule even following enactment of the Durbin Amendment and its implementing regulations.[21] To our knowledge, Mastercard has no such rule.

When a cardholder enters a PIN, the merchant can process the transaction over any of the networks for which the card is enabled (including Visa, since Visa mandated that all issuers must support PIN authentication over the Visa network). By prohibiting merchants from requiring a PIN, Visa is requiring the merchant to cede network choice to the cardholder whenever the issuer has not enabled the competing debit networks' non-PIN authentication features,[22] thereby inhibiting the merchant's ability to route the transaction. In this regard, Visa's actions are similar to its former rules and technical specifications that mandated cardholder selection of the AID and network under the auspices of "cardholder choice." The Federal Reserve found this conduct to be

[19] One reason that merchants must continue to accept Visa and Mastercard is that, due in significant part to their actions, they are the only networks over which non-PIN transactions may be processed. Another is due to the existence of debit cards such as Health Reimbursement Arrangement (HRA) cards that are enabled solely for Visa since they are not covered by the Durbin Amendment. If a merchant stops taking Visa in an effort to avoid the effect of its rules, the merchant will no longer be able to accept HRA and similar exempt cards.

[20] While Visa has argued that this rule is enforced in the interests of "cardholder convenience," this argument is belied by the fact that Visa has no such rule in relation to credit transactions where there is no risk of loss of market share since credit cards are enabled solely for one network.

[21] See Visa Business News bulletin dated September 10, 2015: "To ensure a positive and successful point-of-sale (POS) experience on debit cards, acquirers and their merchants must maintain existing cardholder verification method (CVM) options and follow Visa acceptance guidelines.… For Visa debit acceptance, this includes maintaining the consumer's ability to cancel out of a PIN prompt and instead sign for the transaction if they so choose."

[22] Neither the merchant nor its acquirer is responsible for the issuer's failure to enable the competing debit networks' non-PIN authentication features. If anything, this failure is due to Visa's and Mastercard's conduct described in Sections IV.A-IV.D below.

a violation of the Durbin Amendment and its implementing regulations,[23] as are Visa's actions here.

D. Visa and Mastercard Inhibit Merchant Debit Routing Choice by Refusing to Detokenize In-App Purchases and Card-on-File Transactions, Requiring the Routing of these Transactions to Their Networks

Each credit and debit card possesses a unique 16-digit Primary Account Number ("PAN") assigned by the issuer. This PAN identifies the credit or deposit account to which the card is linked. PANs on cards enabled for Visa generally start with the digit "4," while those enabled for Mastercard generally start with a "5." If a PAN is stolen or otherwise compromised, it often results in fraud and may require the issuer to issue a new PAN and replace the cardholder's physical card. To reduce the chance of the PAN being stolen, and the expensive exercise of replacing cardholders' physical cards, many participants in the payments industry now "tokenize" the PAN.[24]

When a PAN is tokenized, it is replaced with a different 16-digit number ("token") that does not directly correlate to a real account. Visa ordinarily assigns tokens for Visa-enabled debit cards, while Mastercard assigns tokens for Mastercard-enabled debit cards.[25] The cardholder then uses the token at the point of sale or online instead of the real PAN.[26] To the extent a merchant needs to store a cardholder's account number -- for example for recurring monthly transactions -- it can store a token in lieu of the PAN. If the merchant's systems are hacked, the hacker will only gain access to the stored tokens and not the cardholders' PANs. The party that tokenized the PAN (usually Visa or Mastercard) retains a "look-up table" that allows it to convert the token back to its respective PAN ("detokenize") during the payment transaction flow when the token is used for a transaction. This then allows the issuer (which knows the PAN, but not the token) to authorize the transaction.

---

[23] See https://www.federalreserve.gov/paymentsystems/regii-faqs.htm (§ 235.7, Question 4).

[24] In the event that tokens are stolen, they can be immediately deactivated and a new token assigned to each associated PAN. Cardholders do not need to obtain physical replacement cards from their issuers, since the PAN itself (which appears and is encoded on the card) was not compromised. For these reasons, participants throughout the payments industry believe that tokenization is good for issuers, merchants, and cardholders alike, as long as the tokenization process is not used for anticompetitive purposes.

[25] There is nothing proprietary nor technologically advanced about the tokenization or detokenization process, as it merely involves creating a random 16-digit number for tokenization and looking up a correlating PAN on a look-up table to detokenize it. There are tokenization services offered by Visa's and Mastercard's competitors, and merchants regularly use tokenization within their own systems to protect the PAN at various stages of the transaction. However, Visa and Mastercard have each ensured that these competing tokenization services cannot be used by the payments industry throughout the course of a transaction by refusing to process transactions that were tokenized using any competing service. Thus, if a merchant wishes to accept Visa or Mastercard (as most do), they are effectively forced to use Visa's or Mastercard's tokenization services.

[26] This process may be invisible to the cardholder. For example, when a cardholder loads a debit card onto their iPhone through Apple Pay, only a tokenized PAN is retained on the phone. When the cardholder then presents their iPhone for payment at a merchant, the cardholder is unaware that they are actually presenting a tokenized PAN.

Visa and Mastercard have refused to detokenize transactions processed over competing networks where the transaction was made online through a smart phone application[27] or where the merchant retains the token on file for recurring transactions.[28] Therefore, merchants cannot route these transactions to the competing debit networks, since Visa and Mastercard refuse to detokenize the PAN and also refuse to provide these networks with a copy of the look-up table so that they can detokenize the PAN themselves. Without the actual PAN, the competing network cannot ask the issuer to authorize the transaction. Merchants therefore lose their routing choice on all "in-app"[29] and "card-on-file" transactions where the PAN has been tokenized, in violation of 12 C.F.R. § 237(b).[30] The impact of these restrictions is significant, as the number of tokenized transactions continues to grow exponentially. For example, even when customers physically visit a store to purchase an item, they now often make the actual purchase in advance using an application, thus causing the merchant to lose its routing rights due to Visa's and Mastercard's policy against detokenizing these transactions. Moreover, these restrictions are arbitrary and not dictated by technological limitations, but solely enacted to ensure that these transactions may be routed only to the global networks in violation of the Durbin Amendment and its implementing regulations.[31]

In May 2018, in response to repeated complaints that this conduct violated the Durbin Amendment, Visa agreed to detokenize in-app and card-on-file transactions, but only if the *issuer* of the card expressly requests it. This does not cure Visa's violation of the Durbin Amendment and its implementing regulations, which were enacted to protect merchant routing choice, not issuer routing choice. If an issuer has not made such a request, Visa's continued refusal to detokenize these transactions except by issuer request inhibits merchant choice in

[27] For example, a cardholder using a movie chain's app to purchase a movie ticket, or a ride-sharing app to arrange a ride.

[28] For example, a newspaper or video streaming service that retains the cardholder's tokenized debit card number for monthly subscription charges.

[29] In-app purchases clearly fall within the scope of the debit routing prohibitions contained in the Durbin Amendment and its implementing regulations. *See* See, 76 Fed. Reg. 43410 (Jul. 20, 2011) ("[E]lectronic debit card transactions initiated over the Internet are within the scope of this part."); Official Board Commentary on Regulation II, Comment 7(a)-7, 76 Fed. Reg. 43474-75 (Jul. 20, 2011) ("*Application of rule regardless of form factor.* The network exclusivity provisions in § 235.7(a) require that all debit cards be enabled on at least two unaffiliated payment card networks for electronic debit transactions, regardless of whether the debit card is issued in card form. This applies to any supplemental device, such as a fob or token, or chip or application in a mobile phone, that is issued in connection with a plastic card, even if that plastic card fully complies with the rule.").

[30] To avoid the effect of Visa's and Mastercard's refusal to detokenize card-on-file transactions, some merchants are retaining the actual PAN instead of a tokenized PAN, so that they may preserve debit network choice. The defeats the entire purpose of tokenization and subjects all of the merchant's cardholders to unnecessary risk, solely due to Visa's and Mastercard's detokenization policies.

[31] Visa and Mastercard will each detokenize mobile wallet transactions made on a smartphone at a physical merchant location, but both refuse to detokenize in-app purchases made online. Similarly, each will detokenize an online transaction where the cardholder physically enters their card number and the transaction is processed immediately, but neither will do so if the merchant retains the tokenized card number for ongoing card-on-file transactions. These examples show that Visa's and Mastercard's refusal to detokenize certain transactions does not arise from any physical limitation, but solely an effort to force these transactions to their respective networks.

violation of 12 C.F.R. § 235.7(b). Meanwhile, Mastercard to this day refuses to detokenize in-app or card-on-file transactions under any circumstances, in violation of 12 C.F.R. § 235.7(b).

Additionally, even when Visa and Mastercard agree to detokenize a transaction processed by a competing debit network (e.g., a transaction that is not in-app or card-on-file), rather than providing the network with a copy of their PAN look-up tables, they require the competing debit network to do a "call-out" to the global network before the global network will detokenize a transaction. The information that Visa and Mastercard require as part of the call-out goes far beyond the PAN that is necessary to detokenize a transaction, extending to all transaction-related data including the identities of the issuer and merchant, the merchant's store location, and the amount of each individual transaction. This allows Visa and Mastercard to monitor competitively sensitive data relating not only to the competing debit networks, but also relating to the issuing banks and the merchants whose business they are seeking to win from those competing networks. Despite repeated requests, Visa and Mastercard have not only refused to stop requiring this detailed data, but also have refused to even agree to limit the purposes to which they will use this data.

By requiring call-outs, Visa and Mastercard each also create a bottleneck in the payments system, as each tokenized transaction processed by a competing network must be sent to Visa or Mastercard for detokenization. If Visa's or Mastercard's systems go down -- as Visa's recently did in Europe[32] -- this not only stops transactions from flowing through their own networks, but all other competing networks that rely upon them for detokenization. This poses a major and unnecessary risk to the entire U.S. debit payments system.

E. Visa and Mastercard Created "Check Out" Features that Inhibit Merchant Debit Routing Choice, and are Developing Additional Features that may Further Block Merchants' Access to Other Networks

During the past several years, Visa and Mastercard have each created separate online "checkout" features that allow cardholders to store all of their credit and debit cards in a virtual wallet -- regardless of the networks enabled on the card. Thus, for example, cardholders can store their Mastercard-enabled debit cards in Visa's "Visa Checkout" wallet, even though these cards cannot process Visa transactions. Similarly, Visa cardholders can store their Visa-enabled debit cards in Mastercard's "Masterpass" wallet.

When a cardholder visits an online merchant that supports Visa Checkout or Masterpass and indicates they wish to pay using their virtual wallet, the cardholder is prompted to choose which card in the virtual wallet should be used. Once the cardholder's identity is verified through a password or biometric identifier, the transaction can proceed without the cardholder needing to enter any additional personal information.

[32] *See* https://www.ft.com/content/d95698a2-65b3-11e8-90c2-9563a0613e56 ("Visa's European payment systems back up after outage"), retrieved on June 3, 2019.

In marketing these products, Visa tells merchants that "[f]or your customers, signing up is simple and secure and the button works across all devices, with any major credit or debit card,"[33] Mastercard tells merchants that Masterpass "[a]ccepts the cards your customers already have" and that "[c]ustomers can pay with major debit and credit cards from card issuers around the globe."[34] But neither Visa nor Mastercard discloses that, by enabling the feature, merchants are giving up their debit routing choice on tokenized transactions.

For example, if a cardholder stores a debit card enabled for Visa and the competing PULSE debit network in their Visa Checkout wallet, Visa will by default tokenize the card's PAN when it is first stored. However, Visa then refuses to detokenize the PAN for PULSE or any other network enabled on the debit card, meaning that the transaction may only be processed over Visa. Since these details are not disclosed to merchants by Visa, a merchant that enabled the feature would not know that it had given up its debit network routing choice and that all of its transactions on Visa-enabled debit cards were being sent solely to Visa. The same applies to Mastercard and its Masterpass product.[35]

This inhibition of merchant routing choice is a violation of 12 C.F.R. § 235.7(b).[36] And the situation will soon get markedly worse. EMVCo, co-owned by Visa, Mastercard, and the other global networks, is in the process of developing a technological specification called Secure Remote Commerce (SRC). Once finalized, SRC will allow a consumer to register multiple payment methods on a single profile linked to the consumer's identity, and then use that profile to make payments across multiple platforms. The specification will allow purchases not only on websites, but on all electronic devices including smartphones, tablets, and "Internet of Things" devices.[37] Visa and Mastercard have announced their intention to utilize the SRC specification to create a single joint checkout button that will be marketed to merchants and cardholders as a complete payment solution.[38]

---

[33] *See* https://usa.visa.com/run-your-business/small-business-tools/payment-technology/visa-checkout.html, retrieved on June 3, 2019.

[34] *See* https://masterpass.com/en-us/business.html, retrieved on June 3, 2019.

[35] Similar to Visa's and Mastercard's refusal to detokenize in-app and card-on-file transactions, described in Section III.D above, this is another manner in which Visa and Mastercard are misusing the tokenization process -- intended to enhance security -- for their own anticompetitive ends.

[36] The routing prohibitions contained in the Durbin Amendment and its implementing regulations clearly extend to e-commerce transactions and mobile wallets. See, 76 Fed. Reg. 43410 (Jul. 20, 2011) ("[E]lectronic debit card transactions initiated over the Internet are within the scope of this part."); Official Board Commentary on Regulation II, Comment 7(a)-7, 76 Fed. Reg. 43474-75 (Jul. 20, 2011) ("*Application of rule regardless of form factor.* The network exclusivity provisions in § 235.7(a) require that all debit cards be enabled on at least two unaffiliated payment card networks for electronic debit transactions, regardless of whether the debit card is issued in card form. This applies to any supplemental device, such as a fob or token, or chip or application in a mobile phone, that is issued in connection with a plastic card, even if that plastic card fully complies with the rule.").

[37] Internet of Things devices include consumer devices such as connected vehicles, home automation, wearable technology, appliances, medical devices, and others.

[38] "Visa Inc. and Mastercard Inc., the two largest U.S. card networks, said Wednesday that they're planning to drop their longstanding initiatives to get online shoppers to use dedicated payment buttons. The two payments giants instead want to create a new online option that would amount to a shared single payment button that could succeed

The combined power of both Visa and Mastercard participating in a single checkout solution that operates across all platforms and devices will likely incentivize an increased number of merchants to adopt this feature -- particularly since participation by both networks will make it appear ecumenical in nature. It is also likely that Visa and Mastercard will force merchants to adopt the feature by financially penalizing those that don't, as they financially coerced merchants to install EMV terminals by imposing the EMV liability shift. For example, Visa and Mastercard could charge higher fees to online merchants that do not adopt the jointly-developed payment solution, under the pretense that the merchant's transactions are not as secure.

Since SRC involves the tokenization of transaction, it is anticipated that the joint checkout solution will utilize Visa's and Mastercard's tokenization features for *all* transactions on cards enabled for Visa or Mastercard, which include the vast majority of debit cards in the United States. As discussed in Section III.D above, Visa and Mastercard have used their control over tokenization to inhibit merchant routing, precluding transactions from being routed to the competing debit networks that co-reside on these cards. Critically, to date, neither Visa nor Mastercard has been willing to commit to detokenize SRC transactions processed over the competing debit networks. Due to their refusal to detokenize in-app purchases and card-on-file transactions, there is every reason to believe they will similarly refuse to detokenize transactions processed over the joint checkout button.

If, as expected, Visa and Mastercard utilize the new joint payment solution to inhibit merchant debit routing choice, it will comprise another violation of 12 C.F.R. § 237(b).

IV. VISA AND MASTERCARD MISUSE THEIR MARKET POWER AND ENGAGE IN ANTICOMPETITIVE PRICING PRACTICES TO INHIBIT MERCHANT DEBIT ROUTING CHOICE

Until recently, Visa and Mastercard were the only networks that could process non-PIN authenticated transactions, while the competing debit networks could process only PIN authenticated transactions. Since many transactions could not historically be processed using PIN authentication (*e.g.*, mail order, telephone order, and online sales), these transactions, along with all signature-authenticated transactions, could only be processed over Visa or Mastercard.[39] Transactions such as these that cannot be routed to any network other than a single global network are characterized as "non-routable."

Many of the competing debit networks have recently introduced features enabling them to process transactions without a PIN, instead using alternatives such as signature-authentication

---

the current pay tabs, Visa Checkout and Mastercard Masterpass." "Visa, Mastercard Talk About Cooperating in Online Shopping," The Wall Street Journal, April 18, 2018.

[39] As stated above, until recently, Visa and Mastercard each prohibited issuers from enabling both Visa and Mastercard on a single debit card, so as to avoid competition between the two signature networks. This restriction was changed only with enactment of the Durbin Amendment and its implementing regulations, which prohibited such rules. *See* 12 C.F.R. 235.7(a)(3). Again, however, to date no issuing bank has enabled both Visa's and Mastercard's signature networks on one card.

and no-CVM. With these new features enabled, together with the Durbin Amendment's requirement that each debit card be enabled for two networks, every debit transaction should, in theory, be "routable," meaning that the merchant should be able to exercise its statutory right to choose between at least two independent networks regardless of the form of authentication. However, for these new features to work on a particular debit card, they must first be enabled by the card's issuer. Otherwise, the merchant is still forced to send all signature-authenticated and no-CVM transactions to either Visa or Mastercard, thereby preserving Visa's and Mastercard's respective monopolies over these transactions. Since the vast majority of issuers have not enabled the competing debit networks' signature-authentication features and many have not enabled these networks' no-CVM features, most of those transactions -- which together represent a significant majority of all debit transactions -- remain functionally non-routable.

As described below, it is not mere happenstance that issuers have failed to enable the signature and no-CVM features offered by the competing debit networks. Rather, Visa and Mastercard are exploiting their existing market power in debit and in credit to economically coerce issuers not to enable these competition-enhancing features. The result is that Visa and Mastercard have maintained their existing monopolies over debit transactions, while inhibiting merchant choice in violation of the Durbin Amendment and its implementing regulations.[40]

Not content with having maintained their respective monopolies over non-PIN authenticated transactions by inhibiting issuers from enabling the non-PIN features now offered by the competing debit networks, Visa and Mastercard have gone further. While the number of routable transactions has been restricted due to their actions above, they are further misusing their market power in credit and debit to economically coerce both issuers and merchants to send them routable transactions (for which other networks could compete) or be penalized on the pricing of non-routable transactions.

A. Visa and Mastercard Enter Volume Deals with Issuers that Penalize the Issuers for Enabling Competing Networks' No-CVM and Signature-Authentication Products

Visa and Mastercard each offer financial incentives to issuers that agree to process a pre-set volume of the issuer's debit transactions through their networks. In the event the issuer fails to meet the quota, it may lose the entire incentive. The incentives, in the form of payments to the issuer or discounts on the fees charged to the issuer, are substantial, and issuers are thus highly incentivized to meet their quotas. There are indications that Visa and Mastercard have also conditioned issuers' *credit* pricing on the issuer meeting its *debit* volume quotas, thus posing an even greater financial threat to the issuer in the event it fails to meet its debit quota. Visa and

[40] In deciding to require that each debit card be enabled for two unaffiliated networks, instead of requiring that each card be enabled for two unaffiliated networks for each form of authentication, the Federal Reserve noted that one basis for its decision was that the competing debit networks were developing features that would allow them to process non-PIN transactions over their respective networks. *See* 76 Fed. Reg. 43448 (Jul. 20, 2011). As described below, Visa and Mastercard are now undertaking efforts to ensure that these features are not rolled out, thus defeating the rationale relied upon by the Federal Reserve.

Mastercard set these debit quotas at or near the issuer's total signature debit volume, or even its total debit volume.

Issuers know that if they enable the competing debit networks' signature authentication features, merchants will suddenly be able to route signature debit transactions over the less-expensive debit networks enabled on the card. These competing debit networks may also provide superior per-transaction economics to the issuers. However, if merchants do so, it may cause the issuer's Visa or Mastercard debit volume to fall below the quota. The only way for issuers to avoid this is to *not* enable the signature authentication and No-CVM features offered by the competing debit networks, thus forcing merchants to continue to route all signature-authenticated transactions to Visa or Mastercard.

The result is that, notwithstanding the fact that competing debit networks now have signature-authentication features, very few issuers have enabled these features. For the vast majority of cards, merchants still must route all signature transactions over the single global network for which the card is enabled. For the same reason, many issuers have not enabled the competing networks' no-CVM features, thereby requiring merchants to continue routing all no-CVM transactions to Visa or Mastercard. In the absence of Visa's and Mastercard's actions incentivizing the issuer *not* to enable these features, the merchant could route signature and no-CVM transactions over any of the networks enabled on the card. Visa's and Mastercard's conduct has taken away the merchant's ability to do so and therefore violates 12 C.F.R. § 235.7(b). This conduct also separately violates § 12 C.F.R. 235.7(a)(3), because it inhibits the issuer's ability to contract with other networks.

Noting that the Official Board Commentary on Regulation II, provides that an issuer may comply with 12 C.F.R. § 235.7(a)(1) by enabling only one signature-based network and one unaffiliated PIN-based network,[41] Visa and Mastercard may argue that an issuer that succumbs to their actions and blocks signature-authenticated transactions on the competing debit network for which the card is enabled is nonetheless compliant with the Durbin Amendment and its implementing regulations. However, the Official Board Commentary does not condone blocking an alternative form of authentication supported by one of the networks for which the issuer has chosen to enable the card. To the contrary, it expressly provides that "[a]n issuer or payment card network is prohibited from inhibiting a merchant's ability to route or direct an electronic debit transaction over any of the payment card networks that the issuer has enabled to process an electronic debit transaction for that particular debit card."[42] And it certainly does not provide any protection for a network that incentivizes or coerces an issuer into blocking transactions that could be processed on a competing network. Any network that engages in such conduct is, through its actions, causing the number of payment card networks on which a transaction may be processed to less than two unaffiliated networks in violation of 12 C.F.R. § 235.7(a)(1),[43]

---

[41] *See* Official Board Commentary on Regulation II, Comment 7(a)-1, 76 Fed. Reg. 43474 (Jul. 20, 2011).
[42] *Ibid*.
[43] 12 C.F.R. § 235.7(a)(1) broadly prohibits any conduct by a network that "directly or through any … licensed member of the network, by contract, requirement, condition, penalty, or otherwise, restricts the number of payment card networks on which an electronic debit transaction may be processed to less than two unaffiliated networks.

inhibiting merchants from processing transactions over the competing network in violation of 12 C.F.R. § 235.7(b),[44] and inhibiting issuers from contracting with competing networks in violation of 12 C.F.R. § 235.7(a)(3). Moreover, any issuer that succumbs to this conduct, and blocks a form of authentication supported by one of the networks on their cards, is similarly in violation of 12 C.F.R. § 235.7(a)(1) and 12 C.F.R. § 235.7(b).

B. Mastercard Charges Issuers a "Volume Assessment Fee" When Merchants Choose to Route Transactions over Competing Networks, Incentivizing Issuers to Inhibit Merchants' Routing Options

Mastercard charges issuers a compulsory "Volume Assessment Fee" whenever a merchant routes a transaction over a competing (non-Mastercard) network. This fee was 0.2 basis points until July 2016, when Mastercard raised it 15-fold (1,500%) to 3.0 basis points.

Mastercard claims the fee is justified since Mastercard purportedly provides certain services for transactions processed over competing networks. But there is no evidence that the purported services are necessary or helpful to facilitate transaction processing over competing networks, or that any issuer, much less all issuers, want Mastercard to provide these services on transactions processed over these networks. There is no method by which an issuer can opt-out and avoid paying the fee. Moreover, the issuer is already charged a fee by the competing debit network that actually processes the transaction. Mastercard's non-voluntary "Volume Assessment Fee" effectively requires issuers to pay two network fees on such transactions -- one to the network that is processing the transaction, and one paid involuntarily to Mastercard.

The only way for the issuer to avoid paying two sets of network fees is to inhibit transactions from being processed over the competing debit networks. Since all networks support PIN authentication, the issuer does not have control over the merchant's ability to route PIN transactions to the network of its own choice. But, by not enabling the competing debit networks' signature and no-CVM features, the issuer can ensure that the merchant must at least send all signature and no-CVM transactions using Mastercard-enabled cards to Mastercard. By inhibiting the merchant's routing ability for these transactions, the issuer can limit the number of transactions processed over competing networks, and thus limit the instances in which it is paying two sets of network fees. It is significant that Mastercard increased its Volume Assessment Fee 15-fold around the same time that the competing debit networks started rolling out their signature-authentication features, since the effect of the fee is to block merchants' access to these competing services.

Mastercard is incentivizing issuers to inhibit merchant routing choice in violation of 12 C.F.R. § 235.7(b), which prohibits networks from directly or through an issuing bank, by contract, requirement, condition, penalty, or otherwise, inhibiting the merchant's routing choice. Mastercard's Volume Assessment Fee also violates 12 C.F.R. § 235.7(a)(3), because forcing

[44] 12 C.F.R. § 235.7(b) broadly prohibits any conduct by a network that "directly or through any … licensed member of the network, by contract, requirement, condition, penalty, or otherwise," inhibits the ability of a merchant to route a transaction over any of the networks enabled on the card.

issuers to purchase certain services from Mastercard for transactions processed over competing networks inhibits the issuer's ability to contract with these other networks for these services.

C. Mastercard Enters into Signature-Authentication Exclusivity Contracts with Issuers, Ensuring that Merchants Must Continue to Process All of Their Signature-Authenticated Transactions Over Mastercard

Although the Durbin Amendment and its implementing regulations explicitly prohibit exclusivity agreements, Mastercard continues to enter contracts requiring issuers to agree to "100% Mastercard signature debit exclusivity." These contracts expressly bar the issuer from enabling any signature-authentication features offered by the competing debit networks, enabling Mastercard to maintain its complete monopoly over signature-authenticated transactions on these issuers' cards.

When asked to justify this conduct, Mastercard has taken the position that as long as an issuer's debit cards are enabled for one signature-based network and one PIN-based network as required by 12 C.F.R. § 235.7(a)(1) and (a)(2), Mastercard's signature-exclusivity requirements do not violate the Durbin Amendment or its implementing regulations per the Official Board Commentary on Regulation II.[45] But, as described in Section IV.A above, the Official Board Commentary does not condone blocking an alternative form of authentication supported by either of the networks for which an issuer has enabled the card, and it certainly does not provide any protection for a network that incentivizes or coerces an issuer into blocking transactions that could otherwise be processed on a competing network. Mastercard's signature debit exclusivity contracts with issuers are causing the number of payment card networks on which a transaction may be processed to less than two unaffiliated networks in violation of 12 C.F.R. § 235.7(a)(1), inhibiting merchants from processing transactions over the competing network in violation of 12 C.F.R. § 235.7(b), and inhibiting issuers from contracting with competing networks in violation of 12 C.F.R. § 235.7(a)(3). Moreover, any issuer that agrees to these terms is similarly in violation of 12 C.F.R. § 235.7(a)(1) and 12 C.F.R. § 235.7(b).[46]

D. Visa and Mastercard Tie the Pricing of "Routable" Debit Transactions to "Non-Routable" Transactions, Financially Forcing Merchants to Forfeit Network Choice on "Routable" Debit Transactions

As a result of the Durbin Amendment and the signature-authentication and no-CVM features developed by the competing debit networks, there is a potential for every debit transaction to be "routable," meaning that merchants could exercise their statutory right to choose between at least two unaffiliated debit networks for the routing of each transaction. As described above, Visa and

[45] *See* Official Board Commentary on Regulation II, Comment 7(a)-1, 76 Fed. Reg. 43448, 43474 (Jul. 20, 2011).
[46] While we are unaware of any similar "signature exclusivity" contracts entered into between Visa and issuers, there is documented evidence of several instances in which Visa has approached issuers in an effort to dissuade them from enabling the signature authentication and no-CVM features offered by competing debit networks. To the extent any issuing bank responded to Visa's encouragement, Visa's and the issuer's conduct would each violate 12 C.F.R. § 235.7(a) and § 235.7(b) for the reasons described above.

Mastercard have taken numerous anticompetitive actions, in violation of the Durbin Amendment and its implementing regulations, to slow the industry's adoption of these competing signature authentication and no-CVM features. This has enabled the global networks to ensure that a significant majority of debit transactions remain "non-routable," meaning that the merchant is only able to route these transactions to the single global network for which each debit card is enabled -- either Visa or Mastercard.

Having maintained significant debit market power by improperly ensuring that most transactions remain non-routable, and controlling the price over such transactions, Visa and Mastercard have then abused this power in negotiating pricing deals that require the merchant to send Visa or Mastercard a certain volume or quota of their *routable* debit transactions to receive preferential pricing on their *non-routable* transactions. If the merchant falls short of its quota, it loses its preferential pricing for *all* Visa or Mastercard transactions, potentially including credit transactions,[47] resulting in a significant financial penalty. Through these actions, Visa and Mastercard ensure that they not only receive the merchant's non-routable debit transactions, but its routable transactions as well.[48]

If challenged regarding this practice, Visa and Mastercard may argue that merchants must still be financially benefiting from these deals if they are voluntarily entering into them. But that is a myopic view of the situation. Were it not for Visa's and Mastercard's anticompetitive and illegal actions described above, merchants would have routing choice over *all* debit transactions. This would allow a merchant to negotiate effectively with all competing networks, both global and regional, enter into incentive deals with the networks offering the best package deal on pricing, or instead route on a transaction-by-transaction basis to the network offering the best pricing. By artificially and unlawfully maintaining the number of non-routable debit transactions through their actions described above, thereby minimizing the number of transactions that may be sent to competing networks, Visa and Mastercard have precluded merchants from doing either of these things, eliminating the competition contemplated by the Durbin Amendment and its implementing regulations. While it may be true that, in the anticompetitive debit market created by the global networks, merchants are better off by entering incentive deals with Visa or Mastercard, the fact remains that merchants are nonetheless worse off than they would be in a truly competitive market -- where the requirements of the Durbin Amendment and its

[47] While beyond the scope of this memorandum, there are also indications that Visa and Mastercard have tied the pricing of transactions on their respective credit products to the pricing of debit transactions, thus using their dominant market power in credit to financially compel merchants to send routable debit transactions to them rather than to competing networks.

[48] A separate but related manner in which Visa uses its market power over non-routable transactions to divert routable transactions is through its Fixed Acquirer Network Fee ("FANF"). This fixed fee -- implemented by Visa following enactment of the Durbin Amendment in an effort to circumvent it -- is payable by each merchant, through their acquirer, for the mere right to accept Visa transactions. Visa then uses the proceeds from FANF to subsidize per-transaction fees for routable transactions at the back end. Since a significant number of debit transactions are non-routable, Merchants are required to pay the FANF since they cannot refuse to accept Visa. They are therefore being forced to subsidize the back-end per-transaction fee for their own transactions. And, having effectively already paid a portion of their Visa transaction fees through this up-front payment, it does not make economic sense for them to route the transaction over a competing network.

implementing regulations were met and each network could compete for each of the merchant's transactions.

Visa and Mastercard may further assert that the Durbin Amendment permits them to enter debit routing incentive deals with merchants. And there would in fact be no violation of the Durbin Amendment or its implementing regulations if Visa or Mastercard were simply offering the merchant a financial incentive for sending them routable transactions. But this type of permissible conduct is not what is occurring. Visa and Mastercard are, through their actions set forth above, artificially maintaining a high volume of non-routable transactions, and then using their market power over such transactions to force the merchant to give up routing control over the few routable transactions that it could potentially send to competing networks. Through these actions, Visa and Mastercard are inhibiting the merchant's choice of network with regard to these routable transactions, in violation of 12 C.F.R. § 235.7(b).

V. CONCLUSION

Visa and Mastercard have maintained their respective monopolies by taking the actions described above and depriving merchants of debit network routing choice. The Federal Trade Commission, which has exclusive regulatory jurisdiction over network violations of the Durbin Amendment and its implementing regulations, should take action to stop these violations.