August 11, 2021

VIA EMAIL

Ann E. Misback
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551

Re: ***Comments on Regulation II; Docket No. R–1748, RIN 7100–AG15***

Ms. Misback:

The National Retail Federation (NRF) is the world's largest retail trade association. Its members include department stores, specialty, discount, catalog, internet, and independent retailers, chain restaurants, grocery stores, and multi-level marketing companies. Members also include businesses that provide goods and services to retailers, such as vendors and technology providers. NRF represents the largest private-sector industry in the United States that contains over 3.8 million retail establishments, supporting more than 52 million employees contributing $2.6 trillion annually to GDP.

Nearly all the NRF's members accept payment cards, and the fees paid to payment networks and card issuers represent a major expense for each of these retailers. Just as our own members compete against each other for business, with competition driving down prices and increasing quality, the NRF is confident that free competition in the payment space would also result in benefits for each of the stakeholders in the system, including not only retailers but their employees and the customers they serve. However, for decades now, such competition has been elusive as Visa and Mastercard – the dominant networks in both credit and debit – have time and again taken aggressive action to ensure that any opportunity for competition was quashed.

When enacted, Regulation II was intended to introduce competition into the otherwise noncompetitive – or anticompetitive – debit market. In addition to implementing a cap on the amount of interchange that regulated issuers could charge merchants, thereby restricting Visa's and Mastercard's ability to use merchants' money to compete amongst themselves for banks' card-issuing business, Regulation II implemented two critical requirements with respect to debit routing. First, each issuer was required to enable each of its debit cards for two unaffiliated debit networks. Second, issuers and networks were precluded from inhibiting merchants from routing debit transactions over any of the networks for which a card was enabled. In theory, particularly as Visa's and Mastercard's competitors such as STAR, ACCEL, PULSE, NYCE, and SHAZAM (the "Competitive Networks") developed products allowing them each to process all types of transactions--including card not present transactions--merchants should today have at least two debit networks available for virtually every one of their debit

NATIONAL RETAIL FEDERATION
1101 New York Avenue, NW, Suite 1200
Washington, DC 20005
www.nrf.com

transactions. But, as the Board has acknowledged,[1] that is not the case. In particular, merchants' ability to route card not present (CNP) transactions over any network other than Visa or Mastercard remains severely curtailed. Moreover, even with respect to card present transactions, the promise of Regulation II has not come to pass.

The primary reason for merchants' inability to choose between at least two debit networks for each transaction is explained by the actions taken by Visa and Mastercard since Regulation II was enacted. These actions, described in detail in a white paper prepared by the NRF for the Federal Trade Commission,[2] were taken for the express purpose of ensuring that Visa and Mastercard could retain their respective control over the routing of debit transactions. In executing this plan, Visa and Mastercard flaunted Regulation II, distorting its language in ways that purportedly allowed them to pursue their efforts to quash merchant debit routing choice.

At the outset, we note and emphasize that the NRF is strongly supportive of the Board's efforts to amend Regulation II for the purpose of clarifying that its prohibitions extend to card not present transactions. In the NRF's view, this was clear on the face of Regulation II when it was first enacted, and the only reason this clarification is necessary is due to the intentional misinterpretation of its original language by Visa and Mastercard. But NRF is concerned that unless the Board's clarification of the scope of Regulation II is ironclad and not subject to ambiguity, its work may prove to have been for naught in future years because Visa and Mastercard are likely to take advantage of any loopholes they may read into the new language.

Having reviewed the Board's proposed amendment to Regulation II, the NRF is particularly concerned about three ways in which the language of these amendments may be distorted and thus subvert the Board's intention to provide routing choice to merchants for each transaction: [1] cardholder authentication, [2] tokenization, [3] issuer volume incentive deals, and [4] AID prioritization.

Method of Cardholder Authentication:

In enacting Regulation II, the Board was required to decide whether to require two unaffiliated networks per card, or two per form of cardholder authentication.[3] At that time, the primary means of authenticating a cardholder's identity were signature and PIN, so the essential question addressed by the Board was whether there needed to be two networks available to merchants for both signature and PIN transactions at the point of sale.

The Board ultimately decided to require two networks per card, rather than requiring two networks for each form of cardholder authentication. Among the reasons identified was that the competitive networks were developing technology that would allow transactions to be processed over their networks without the need for a PIN.[4] If this were the case, then merchants would have a choice of

[1] Federal Register, Vol. 86, No. 91, p. 26190 ("Despite these developments, and in contrast to the routing choice that currently exists for card-present transactions, merchants are often not able to choose from at least two unaffiliated networks when routing card-not-present transactions, according to data collected by the Board and information from industry participants.")
[2] A copy of the white paper prepared by the NRF is publicly available on the Federal Reserve website at https://www.federalreserve.gov/regreform/rr-commpublic/merchant-network-meeting-20190611.pdf.
[3] The issue considered by the Board related solely to cardholder authentication. In other words, the method through which the identity of the cardholder would be verified. The Board did not consider whether methods of authenticating the card *itself* could be used to thwart merchant routing choice. That issue is discussed below in the section relating to tokenization of the Primary Account Number.
[4] Federal Register, Vol. 76, No. 139, p. 43448 ("The Board further understands that there exist emerging PIN debit products and technologies that would allow PIN debit to be used in additional retail environments where PIN debit

two networks on PIN transactions (since Visa, Mastercard, and each of the competitive networks were enabled for PIN transactions), along with signature transactions or other types of transactions authenticated without a PIN, including card-not-present (CNP) transactions (once the competitive networks rolled out their these new cardholder authentication features).

The competitive networks did, in fact, develop the technology necessary to process transactions without a PIN, and all of the competitive networks have had this capability for several years.[5] But issuers, by and large, have not enabled their cards to support these features, leaving Visa or Mastercard as the sole network on their cards that can process CNP transactions. This is not occurring because of technological challenges in enabling non-PIN processing. In fact, for at least several of the competitive networks, issuers must take affirmative steps to *disable* these features, as they are otherwise automatically enabled by the network.

There are two reasons that issuers have disabled these features, thereby precluding merchants' routing choice for CNP transactions. First, Visa and Mastercard provide incentive payments to issuers structured in a way that, if the issuer enables the competitive network's CNP features, it will lose its incentive. As a result, issuers actively disable these features, requiring merchants to route all CNP transactions to Visa or Mastercard – even if more expensive for the merchant – so that the issuer can collect its incentive payment. Second, with respect to smaller, unregulated merchants, Visa and Mastercard offer the promise of higher interchange, encouraging the issuer to disable the competitive network's CNP functionality.[6] This results in higher profits for the bank as merchants are forced to pay them higher interchange rates, awarding the bank for having affirmatively disabled the competitive networks' CNP functionality.[7]

---

is not generally offered, such as for online purchases. Some billers and at least one online merchant accept transactions that are routed over PIN debit networks, without requiring the cardholder to provide his or her PIN. The Board anticipates that the elimination of network and issuer-based routing restrictions may further promote innovation to facilitate the use of PIN debit in additional retail environments.")

[5] E.g., STAR ACCESS (STAR network), ANP+ (ACCEL network), PULSE PAY Express (PULSE network), Sure Pass and Elite Pass (SHAZAM network), NYCE PINless POS (NYCE network).

[6] To date, hundreds of unregulated banks have submitted comments to the Board regarding the proposed amendments to Regulation II. Each of these acknowledges that a primary reason for the banks' objection to the proposed amendment is the loss of revenue. These issuers cynically complain that – if merchants are in fact granted the routing choice intended by Regulation II – they will no longer be able to profit from the increased interchange charged to the merchants due to Visa's and Mastercard's bloated interchange rates. Instead, these issuers are asking that the Board leave Regulation II as it currently exists, allowing them to continue to force merchants to route each CNP transaction over a single network – either Visa or Mastercard – each of which costs the merchants more and results in increased profits to the bank.

[7] The letters submitted by the unregulated banks relatedly complain that the Board's proposed rule "does not mention that the U.S. Supreme Court found in 2017 that the card market is a two-sided one, where policymakers must balance the commercial interests of issuers and merchants." Yet the only 2017 Supreme Court case involving credit cards, *Expressions Hair Design v. Schneiderman*, 137 S.Ct. 1144 (2017), did not at all discuss two-sided markets. In fact, the decision awarded merchants a win, holding that a New York law prohibiting a merchant from listing a retail price and a separate fee for use of a credit card constitutes a regulation on commercial speech. *Id.* at 1151. In discussing the interchange fees paid by merchants, the Court correctly noted that "[t]hose fees add up…" *Id.* at 1148. Perhaps the letter instead intended to refer to *Ohio v. American Express Company*, 138 S.Ct. 2274 (2018), a case the following year which did involve two-sided markets. But if so, its summary of the case is plainly incorrect. The Supreme Court was deciding an antitrust case about credit cards and did not direct "policymakers" to do anything, let alone imply that any statute or regulation should be modified. Nor did it mention a balancing between the interest of issuers and merchants. Instead, it directed that, in analyzing the two-sided credit card "transactions" market, courts must balance the interests of merchants and *cardholders. Id.* at 2286 ("Thus, courts must include both sides of the platform—merchants and cardholders—when defining the credit-card market."). The Court also observed that "Visa and MasterCard have significant structural advantages" over American Express, including the fact that nearly all banks are members of either or both of Visa and Mastercard.

Meanwhile, ecommerce transactions, which were growing quickly but still comprised a small share of overall commerce at the time the original Regulation II was enacted, have since grown (and continue to grow) exponentially. Since these are CNP transactions, this means that the issuers' gamesmanship with cardholder authentication enablement, as incentivized by Visa and Mastercard, has a significant impact on merchants that continues to increase. The competitive networks have found a way to technically facilitate merchants' routing choice – as the Board anticipated. But, because of the actions of actions of Visa, Mastercard, and the issuers, merchants today are generally still left with only one network – Visa or Mastercard – for signature and other non-PIN-authenticated transactions, including CNP transactions.[8] Meanwhile, Visa, Mastercard, and the issuers have continued to profit from their elimination of merchant routing choice, further enriching themselves at the expense of merchants, and ultimately consumers.[9]

It appears to the NRF that the Board's proposed rule attempts to rectify this situation by requiring that two networks be made available by the issuer for all types of transactions. This would include CNP transactions, including ecommerce transactions. The proposal would, in theory, require issuers to enable CNP cardholder authentication methods for at least two unaffiliated networks on their cards. We think this is a significant step forward, and warmly welcome it.

But the Board did not explain how this requirement overlaps with the concept of cardholder authentication. We believe that, without further clarification, this provides a loophole through which the Board's current efforts may be negated. Specifically, in the same way that Visa, Mastercard, and the issuers took advantage of the Board's decision not to require two networks for each form of cardholder authentication in the past we fear that, in the absence of guidance on this issue, they will once again rely on authentication as a method through which to destroy merchant routing choice.

For example, if a third-party service provider launches a form of cardholder authentication that is neither secure, convenient, efficient, nor economical, an issuer could claim this loophole allows it to enable the competitive network *only* for that obscure (and inherently noncompetitive) form of cardholder authentication, while enabling Visa and Mastercard for all forms of cardholder authentication.[10] As long

---

This horizontal "structural advantage"—the fact that Visa and Mastercard manage a cartel of issuing banks—is currently the focus of antitrust litigation unrelated to the *Amex* case.

[8] Unlike the signature vs. PIN dichotomy in the original Regulation II, this is not a situation in which merchants can preserve their routing choice simply by purchasing a PIN pad, as there are no widely-accepted methods to authenticate CNP transactions by use of a PIN. There is nothing merchants can do to obtain the network choice for CNP transactions that had been taken away from them by the issuer's disablement of the competitive networks' CNP authentication products.

[9] In its comment letter dated July 23, 2021, Visa asserts that the non-adoption of the competitive networks' CNP cardholder authentication features is perhaps because "merchants simply might not feel they need such options." *Id.* at n.4. Laying any blame for such non-adoption at the feet of merchants is wholly disingenuous. Merchants of course have a strong desire for a second unaffiliated network over which they can choose to process CNP transactions. But merchants cannot do so unless the competitive networks' CNP features are enabled by the issuer. And these features are disabled due to Visa's and Mastercard's incentive payments and the desire of unregulated issuers to collect inflated interchange at the expense of merchants. Visa similarly claims that the competitive networks have not sufficiently incentivized issuers to enable the competitive networks' CNP features (or, more accurately, not to disable these features). But the competitive networks should not be required to dissuade issuers from blocking routing choice through the disablement of these networks' CNP features. Nor should the availability of a second unaffiliated network for the routing of CNP transactions be contingent upon the results of a bidding war between the global networks that are trying to preclude merchant routing choice and the competitive networks that are attempting to preserve it.

[10] Visa or Mastercard could incentivize the issuer to do this, as they do today. Alternatively, an unregulated issuer might do this of its own volition to increase the number of transactions processed over Visa and Mastercard as

as card-present and CNP transactions can *theoretically* be routed using this new form of cardholder authentication, the issuer could claim it remains compliant with the Fed's proposed new rules, even though merchants would then be forced to use that inferior and expensive form of cardholder authentication if they wished to preserve their routing choice. Merchants should not be put to this Hobson's choice.

Similarly, Visa or Mastercard could incentivize an issuer to enable the full suite of cardholder authentication methods for their network, but to disable PIN cardholder authentication for the competitive network on the card. This would arguably comply with the new proposed rule, as the two PINless networks would be available for both card present and CNP transactions. But it would force merchants to route all PIN transactions (which are overwhelmingly card-present) to Visa or Mastercard. Merchants would need to choose between the increased security offered by PIN transactions or forfeit this security to obtain routing choice. Again, merchants should not be put to this false "choice."

These are only two potential scenarios. As we have seen, based upon their past conduct, the creativity of Visa and Mastercard is boundless when it involves protecting their market share and inhibiting merchant debit network choice.

We believe that there is a simple remedy for this. Issuers should be allowed to choose the unaffiliated networks they enable on their cards, as long as they ensure that there are two unaffiliated networks available for *each type* of transaction. As a logical extension of this principle, they should also be required to enable all forms of cardholder authentication that are offered by the networks they have chosen. The Board should clarify that partial enablement of a network – whereby one or more of its forms of cardholder authentication is disabled by the issuer – does not meet the requirement of enabling two unaffiliated networks for each type of transaction.

Alternatively, or in addition, to the extent an issuer chooses to enable a particular form of cardholder authentication on their cards, they should be required to enable that form of cardholder authentication for all networks on the card, but only to the extent supported by those other networks. Thus, for example, if an issuer chooses not to enable biometric cardholder authentication, it need not do so for any network on the card. But if it chooses to enable that form of cardholder authentication for one network, it must enable it for all networks enabled on the card, if offered by those networks.

Failing to incorporate one of these solutions, or otherwise closing the cardholder authentication loophole, runs the risk of cardholder authentication being used to circumvent the Durbin Amendment – the exact conduct which has already occurred and which the Board is presumably attempting to address through its proposed amendments.

Neither of these solutions runs contrary to the Board's earlier decision not to *require* two networks for each form of cardholder authentication available to merchants, as neither imposes that requirement. As such, the Board need not retract its earlier decision. Similarly, neither solution inhibits the technological development of innovative new forms of cardholder authentication. If only one network develops a new innovative technology, and it is not available on other networks, issuers can enable it for that one network without running afoul of either of these proposed solutions.

Moreover, both solutions are consistent with and supported by the language of Regulation II. Regulation II requires that, for a network to count as one of the two unaffiliated networks required by law, the network must have "taken steps reasonably designed to be able to process the electronic debit

---

compared to the competitive network, awarding the issuer with increased interchange at the expense of the merchant which has lost their routing choice.

transactions that it would reasonably expect will be routed to it…" 12 C.F.R. § 235.7(a)(2). Here, the competitive networks have attempted to take such steps – they have created new forms of cardholder authentication that permit CNP transactions to be routed to them. But the issuers have negated these required steps by refusal to enable these features. As a result, the competitive network on the card is not "able to process the electronic debit transactions that it would reasonably expect will be routed to it." In these circumstances, the issuer should be deemed not to have enabled the network for purposes of complying with 12 C.F.R. § 235.7(a)(2) either in its original form, or in its proposed amended form. No amendment to 12 C.F.R. § 235.7 is required to adopt either or both of these solutions; only an explanation in the Official Commentary.[11]

Tokenization

Tokenization is a process through which the Primary Account Number (PAN) – the 16-digit number that ordinarily appears on a physical debit card – is translated into a different 16-digit number called a token. Just like the PAN is a 16-digit number that points to the depositor's bank account number, the token is a 16-digit number that points to the PAN.

One major benefit of using a token is that, if the token is compromised, the old token may be cancelled, and a new token issued those points to the same PAN. There is no need to replace the PAN itself and thus no need to issue a new physical debit card. Similarly, if a group of tokens are compromised, they may all be deactivated and reissued without any physical card reissuance. NRF has no opposition to tokenization itself; in fact, it strongly supports it as a security measure.

Visa and Mastercard each offer tokenization services through which they translate PANs into tokens. They each have a look-up table which lists each PAN and the corresponding token, which they do not share with anyone. As such, once Visa or Mastercard tokenize a PAN, no one else is able to detokenize it. Virtually every debit card issuer in the United States uses Visa's or Mastercard's tokenization services. Thus, for example, if a cardholder loads their debit card onto their phone, the PAN itself is not stored on the device. Rather, it is a token that has been provisioned by either Visa or Mastercard at the issuer's request. When that token is then presented to a merchant, the transaction cannot be processed until it is detokenized back into a PAN by whichever of the two networks that tokenized it. If the transaction is processed over Visa or Mastercard, they may detokenize it as they process it in the ordinary transaction flow. But if the transaction is to be processed over the competitive network for which the card is enabled, the token must first be detokenized by Visa or Mastercard. Visa and Mastercard therefor have the ability to block any transactions on a tokenized card – tokenized by them as a result of a contract with the card issuer – from being processed over any other network. And both have abused this power in different ways.

Specifically, when a merchant chooses to route a transaction over a competitive network, Mastercard is arbitrarily selective about whether it is willing to detokenize the PAN. If the transaction is a

[11] In its comment letter dated July 23, 2021, Visa asserts that the Board need not take action in relation to the issuers' disablement of the competitive networks' CNP functions, since the market will take care of this over time. *Id.* at p. 4. Considering that issuers continue to receive incentives from Visa and Mastercard to disable these features, and unregulated issuers further collect increased interchange from their disablement, there is no reason to believe that the market will ever cure this problem. In support of this argument, Visa also asserts that when it introduced signature debit in the 1990s, it needed to go issuer by issuer to convince them to add signature debit functionality. But Visa did not convince issuers to adopt its signature debit product by going door-to-door. Rather, it did so by offering issuers significantly higher interchange in relation to signature debit transactions, and it then forced the merchants to accept those transactions–and pay these higher rates–through its "honor all cards" rule that linked credit and debit acceptance.

CNP transaction, Mastercard refuses to detokenize the transaction, taking away the merchant's routing choice. By virtue of Mastercard's refusal, these transactions are only routable to Mastercard.

Visa goes about using tokens to inhibit merchant routing choice a different way. When a token is detokenized, there are two security checks run – confirmation of the cryptogram and domain channel – to ensure that the token is valid. Issuers require that the network processing the transaction confirm that these security checks have been successfully performed before the issuer will authorize a transaction. Knowing this, when a competitive network requests that Visa detokenize a CNP transaction in particular, Visa will provide the PAN, but it will not confirm whether the token was validated. The result is the same as with Mastercard's policy: the transaction may only be routed to one network – this time, Visa.

Notably, Visa and Mastercard act this way *only* when the merchant attempts to route a CNP transaction to a competitive network. Visa and Mastercard are willing to fully detokenize all card present transactions, including provision of the cryptogram and domain channel authentication. But when it comes to CNP transactions, on which their iron grip is being challenged, they resort to conduct that protects their historical control over these transactions. There is no security reason for this, and certainly no reason that Visa or Mastercard should be the arbiter of which types of transactions should be blocked. These practices amount to nothing less than a frontal attack on Regulation II and the competition that it was intended to foster. As with their other conduct, it is clear that the focus of their policies is protecting their grip on CNP transactions.

This is not a situation where the merchant chose to use Mastercard's or Visa's tokenization services. To the contrary, it is the issuer that elected to do so, and the PAN is already tokenized by the time it is presented to the merchant. Through no fault of its own, in the absence of direction from the Board, the routing choice of the merchant is subject to Mastercard's and Visa's benevolence.

In NRF's view, the conduct described above violates both the original and newly-proposed language of Regulation II. Specifically, with certain exceptions not applicable here, Regulation II currently defines a "debit card" as:

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.

12 C.F.R. § 235.2(f) (emphasis added).

The current Official Commentary similarly makes clear that:

The term ''debit card'' as defined in § 235.2(f) applies to any card, *or other payment code or device*, even if it is not issued in a physical form. *Debit cards include, for example, an account number or code* that can be used to access funds in an account to make Internet purchases.

Official Board Commentary on Regulation II, 12 C.F.R. § 235.2, 2(f)(1) (emphasis added).

Under both the plain language of Regulation II and that of the Official Commentary, it is clear that a token is a "debit card." And, as a result, any transactions performed using the token must be enabled for processing over at least two unaffiliated networks:

Section 235.7(a) requires a debit card subject to the regulation to be enabled on at least two unaffiliated payment card networks.

Official Board Commentary on Regulation II, 12 C.F.R. § 235.7, 7(a)(1).

Yet notwithstanding this clear language, Visa and Mastercard use their power over tokenization – granted to them by the issuer – to ensure that merchants are only able to route CNP transactions over their own networks.

The Board's proposed revisions to Regulation II contemplate adding language which appears to address this issue, providing:

Application of rule regardless of means of access. The network exclusivity provisions in § 235.7(a) require that a debit card be enabled by the issuer on at least two unaffiliated payment card networks for each means of access. The means of access that carries the debit card information could be a plastic card, a supplemental device such as a fob, information stored inside an e-wallet on a mobile phone or other device, or another means of access that may be developed in the future.

On its face, this proposed language applies to tokenization—the "information" stored inside an e-wallet is, after all, a token. However, just as Visa and Mastercard have ignored the existing language of Regulation II, the NRF has every reason to believe that they will similarly attempt to circumvent this proposed language.

This concern is not mere conjecture. In its comment letter dated July 23, 2021, Visa complains about the Board's proposed language protecting merchant choice regardless of the "means of access" used to access the account, claiming that it should not be adopted since it "may" be read to apply to a one-time passcode generated by a network that is then provided to a cardholder by an issuer. Id. at p. 15. In other words, Visa contends that by inserting this additional step into the transaction process, a network and issuer working in tandem should be permitted to block merchants from accessing the unaffiliated network on the card, and that the Board should not adopt its proposed language since it "may" be read to prohibit such conduct. But this conduct is already prohibited by the existing language of Regulation II, which extends the definition of "debit card" to "any card, or *other payment code*," "*regardless* of whether authorization is based on signature, personal identification number (PIN), *or other means*." 12 C.F.R. § 235.2(f)(emphasis added). The scenario proposed by Visa is not a reason for the Board to change its proposed language clarifying that merchant routing choice applies regardless of the "means of access" used to access the account. If anything, it is reason for the Board to expressly confirm that the conduct in which Visa seeks to engage is a prohibited business practice under either the existing or amended language.

Visa also comes at this issue another way, arguing in its comment letter that the Board's clarification of Regulation II should not extend to "ancillary features that are more properly viewed as components of authentication." Id. at p. 16. Presumably this represents an effort to allow Visa to continue to refuse to provide the cryptogram and domain channel authentication to for transactions that are to be processed over the competitive networks even where the PAN has been tokenized by Visa at the issuer's request. Visa contends that preserving merchant debit routing choice with respect to transactions using these "ancillary features" would run contrary to the Board's determination in enacting the original Regulation II that issuers are not required to enable two unaffiliated networks for each form of cardholder authentication. Id. But Visa conflates authentication of the cardholder's identity with authentication of the card itself. Unlike signature and PIN authentication, the cryptogram and domain channel are not used to authenticate the identity of the cardholder; they are not cardholder verification methods (CVMs). Rather, these are mechanisms required by the issuer to ensure that the debit card itself – in its tokenized form – is authentic. If an issuer requires that a particular method be used to ensure that a tokenized debit card is authentic, as issuers do today by requiring authentication of the cryptogram and domain channel, it cannot then use that requirement to defeat merchant routing choice by selecting as its TSP a network that refuses

to provide this information when the transaction is to be processed over the competitive networks. By doing so, the issuer and network have converted the PAN into a code which is still subject to merchant routing protections, 12 C.F.R. § 235.2(f), but which can no longer be processed over a competitive network.

NRF suggests that the Board clarify the existing language of Regulation II not only by adding its newly-proposed language above, but also through an express requirement that any token provisioned by an issuer, network, or a third party acting on their behalf must be detokenized at the request of any other network for which the card is enabled. Moreover, consistent with the Fed's existing FAQ stating that it is a violation of 12 C.F.R. § 235.7 to "impos[e] an additional cost on the use of a competing payment card network," this should include a requirement that the detokenization be performed at no cost. This will not only protect merchant routing choice as was intended by Regulation II, but also increase security for the payment system as a whole. As noted above, the NRF strongly supports tokenization as a security measure, and the Board's clarification would permit all networks to process tokenized transactions – resulting in increased security while not compromising merchant routing choice or degrading issuers' fraud detection capabilities. Again, this does not require an amendment to Regulation II, as it is wholly consistent with its existing and proposed new provisions. Only a comment from the Board or the identification of Visa's and Mastercard's conduct on this issue as prohibited is required.

Volume-Based Incentive Deals

As discussed above, the major competitive networks have, for several years now, offered features allowing CNP transactions to be processed over their respective networks. If issuers had enabled these features, all debit cards would already be able to process CNP transactions over two unaffiliated networks, and the need for the Board to clarify Regulation II would not have been as great. But many issuers – and in particular larger regulated issuers – have disabled these features as a result of incentives provided by Visa and Mastercard.

Specifically, 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 stands to lose the entire incentive. The incentives, in the form of direct 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.

Issuers know that unless they disable the competitive debit networks' CNP features, merchants will be able to (and will) route CNP transactions over the less-expensive competitive debit networks enabled on the card. If merchants do so, it may cause the issuer's Visa or Mastercard debit volume to fall below the quota, resulting in the loss of their incentive. The only way for issuers to avoid this is to disable the CNP features offered by the competing debit networks, thus forcing merchants to continue to route all such transactions to Visa or Mastercard.

If the Board's proposed rules are enacted, issuers will – in theory – be compelled to enable the competitive network's CNP features so as to provide an unaffiliated network over which these transactions may be processed. But this does not mean that issuers, incentivized by Visa or Mastercard, will not find other schemes involving tokenization, cardholder authentication, misuse of EMV technology, or other methods to inhibit merchants' ability to route transactions to the competitive networks. We have for years witnessed these schemes occurring, and there is no reason to believe they will suddenly stop. The only way an issuer can meet a volume-based incentive offered by one of the global networks is to take actions that will preclude merchants from being able to route transactions over the less-expensive competitive networks. We therefore believe it appropriate for the Board to clarify that

volume-based incentive agreements are not permitted under Regulation II. This is wholly consistent with the language of the existing regulation.

Regardless of the requirements imposed on an issuer by Regulation II when it comes to card enablement, no network should be permitted to incentivize an issuer to take actions that will adversely affect a merchant's choice of 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), 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 succumbs to this conduct, and blocks a form of cardholder 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). And yet, we have seen all of this conduct notwithstanding the clear mandate of Regulation II.

Ultimately, once issuers choose the unaffiliated networks for which their cards are enabled, they should have no control over the percentage of transactions that flow over each of these networks. That decision should rest solely within the discretion of the merchants that accept their cards. After all, preservation of this merchant routing choice from issuer and network interference is one of the primary purposes of Regulation II. But volume-based incentive agreements instead encourage the issuer to do whatever they can to affect the volume that is transacted over the various networks on the card, which they may only do by restricting merchant routing choice. That is, after all, the purpose of a volume-based incentive agreement, and these should be prohibited as violating 12 C.F.R. § 235.7(a)(1), 12 C.F.R. § 235.7(a)(3), and 12 C.F.R. § 235.7(b). There is no need to amend Regulation II to address this issue. However, the Board can and should clarify in its Official Commentary that volume-based incentive agreements are a prohibited business practice under the provisions of 12 C.F.R. cited above.[12]

Misuse of AID Selection

Virtually every physical debit card issued in the United States today contains an EMV computer chip. This chip is 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, while relegating other debit networks to the use of the outdated magnetic stripe. However, Regulation II was then enacted, requiring that Visa and Mastercard allow transactions destined for the competitive networks to be processed using EMV technology. Visa and Mastercard did not want to allow the competitive debit networks to process transactions over their existing Global AIDs, as they did not want to afford equal footing to these networks. Even though EMV technology itself has no effect on transaction routing—which is done by the BIN number—in an effort to appear as if they were complying with Regulation II, Visa and Mastercard agreed to create a separate-but-unequal "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

[12] When this concern was raised during the comment period on the original version of Regulation II, the Board decided not to address it in the final rule on the basis that the issuer's ability to affect routing would be significantly reduced since "merchant routing preferences will take priority over issuer and network routing preferences," and since the competitive network added to the card would need to meet the requirements of § 235.7(a)(1). As we have since seen, issuers, incentivized by the networks, have cleverly avoided these requirements, allowing them to significantly affect merchant routing choice. The NRF is of the view that, given the experiences to date, the Board should reconsider this decision.

global network enabled on the card (either Visa or Mastercard); 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 Mastercard).[13]

Since there are multiple AIDs on U.S.-issued debit cards, making the implementation of EMV more complex, merchants' terminals must be programmed to select from among these AIDs when an EMV card is dipped into the terminal. One of the methods authorized by EMVCo for selection of the AID is to do so based on the "priority" assigned to the AID by the issuer. Accordingly, there are countless point-of-sale terminals already installed at merchant locations throughout the country that select the AID based on the priority assigned to the AIDs by the issuer.

EMVCo's specifications also require the issuer to assign a "priority" to each of the AIDs on the card to facilitate the terminal's selection among them. Knowing this basic design of EMV specs, and the fact that there are myriad terminals that have been programmed to select the AID based on issuer-assigned priority, Visa and Mastercard each enacted rules requiring that all debit card issuers in the United States prioritize the Global AID over the Common AID. As a result, whenever any EMV debit card is used at one of these terminals, the transaction may only be routed to Visa or Mastercard.[14] There is no justification for this prioritization mandate, nor any reason other than suppressing merchant routing choice that would explain prioritization of an AID that can route solely to one network, and it should be prohibited.[15]

Visa and Mastercard have taken the position that merchants who have installed priority-based terminals and want routing choice should either reprogram their terminals or purchase new ones. But many merchants (particularly smaller ones) are unaware that their terminals have been programmed in a way that – *due to Visa's and Mastercard's prioritization mandate* – are taking away their routing choice. Merchants should not be required to police issuers' or networks' compliance with the Durbin Amendment, nor bear the burden of learning the intricacies of EMV technology and how to avoid the effects of AID prioritization rules. Moreover, they certainly should not be required to spend the significant resources required to reprogram their terminals or to purchase new terminals simply to avoid

[13] Even though Visa and Mastercard licensed the Common AID to the competitive networks, the licensing terms nonetheless discriminate against the competitive networks by allowing them to solely process PIN-authenticated transactions or those with no authentication method whatsoever. Visa and Mastercard, by contrast, kept for themselves the Signature CVM and CD-CVM, which is used to convey biometric authentication data to issuers, refusing to license it to the competitive networks and thereby precluding those networks from processing transactions using these forms of authentication.

[14] In its comment letter dated July 23, 2021, Visa asserts that there is no reason to believe that the existing language of Regulation II has been ineffective in protecting merchant routing choice with respect to card present transactions. *Id.* at pp. 6-7. Clearly that is not the case, as many merchants are losing their routing choice on all card present transactions as a result of Visa's and Mastercard's AID prioritization rules which they contend are not prohibited by the existing language of Regulation II.

[15] Visa has in the past asserted that the Global AID must be prioritized since otherwise U.S.-issued debit cards will not work overseas because the Common AID is not recognized there. This is wholly inaccurate. When a EMV card is inserted into a EMV terminal, the terminal builds a "Candidate List" of the AIDs that are both contained on the card *and* recognized by the terminal. When a U.S.-issued debit card is inserted into an EMV terminal overseas, the terminal recognizes only the Global AID, the Candidate List contains only the Global AID, and the Global AID will be automatically selected notwithstanding the existence or prioritization of the Common AID on the card. The only circumstance in which AID prioritization is relevant for a card containing both the Global and Common AIDs is if it is inserted into a U.S. merchant's terminal.

the effects of issuers' prioritization of a non-Regulation II compliant AID that can route only to one network.[16]

In its proposed clarification of Regulation II, there appears to be language that, rationally construed, would prohibit this conduct. Specifically, the proposal identifies as a prohibited business practice:

Establishing network rules or designating issuer priorities directing the processing of an electronic debit transaction on a specified payment card network or its affiliated networks, or directing the processing of the transaction away from a specified payment card network or its affiliates, except as (i) a default rule in the event the merchant, or its acquirer or processor, does not designate a routing preference, or (ii) if required by state law.

However, NRF expects that if this language is enacted as-is, Visa and Mastercard will retain their prioritization rules, arguing – as they have – that by failing to incur the expense of purchasing a new terminal or reprograming their existing terminal, the merchant has chosen not to designate a routing preference. Of course, this is an utter fallacy, as it is not the merchant's terminal but Visa's and Mastercard's prioritization rules followed by the issuers that has given rise to this issue.

The NRF therefore proposes that the Board clarify that the language above requires that issuers prioritize a Regulation II-compliant AID on all debit cards issued in the United States. That is to say, an AID that can route to at least two unaffiliated debit networks, and do so without discrimination against any of those networks such as exists today. Without this additional clarification, the NRF (and the Board) have every reason to believe that Visa and Mastercard will continue to use their control over EMV technology to disadvantage the competitive networks and take away merchant choice.[17]

Updating Regulated Interchange Fees

One important aspect of Regulation II that is not addressed by the Board's proposed revisions is the limitation that is placed upon regulated debit interchange fees. While the NRF recognizes that this is beyond the scope of the proposed revisions, it urges the Board to revisit this issue at the earliest opportunity.

While data collected and published by the Board recognizes that issuer costs have nearly halved from those previously incurred, to less than four cents per transaction,[18] no correlating adjustment has been made to the regulated transaction interchange rates. Similarly, while this same data shows that more

---

[16] Networks and issuers cannot take any action – here prioritizing the Global AID – that requires a merchant or issuer to incur expense to protect its debit routing choice. Board of Governors of the Federal Reserve System – *Frequently Asked Questions About Regulation II* (Debit Card Interchange Fees and Routing), § 235.7, Q2.

[17] To the extent issuers complain about the cost of issuing new debit cards so that a Regulation II-compliant AID is prioritized, there is a simple solution to this. Visa and Mastercard can simply license access to the Global AID to the competitive networks in a non-discriminatory manner. This should have been done at the outset of the EMV rollout, in which case there would have been no need for the Common AID. But Visa and Mastercard refused to do so, enabling them to manipulate AID prioritization and selection as discussed above. Visa and Mastercard should not be heard to complain about this, considering that the existing prioritization scheme is of their own making and EMV technology itself is routing neutral. However, it is not necessary for the Fed to get into these details; it need only clarify that issuers must prioritize a Durbin-compliant AID.

[18] *2019 Interchange Fee Revenue, Covered Issuer Costs, and Covered Issuer and Merchant Fraud Losses Related to Debit Card Transactions*, Board of Governors of the Federal Reserve System (May 2021) at 21, https://www.federalreserve.gov/paymentsystems/regii-data-collections.htm.

of the expenses relating to fraud have been shifted to merchants,[19] with issuer incurring reduced fraud-related expenses, no revisions have been made to account for this.

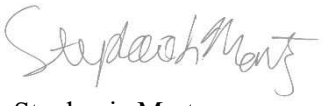
To ensure that regulated debit interchange is "reasonable and proportional to the cost incurred by the issuer with respect to the transaction," as required by the Durbin Amendment,15 U.S.C. § 1693o-2(a)(2)-(3), these changed circumstances should be addressed by the Board and the permissible regulated interchange rate adjusted downward accordingly.

Conclusion

By issuing its proposed revisions to Regulation II, the Board has taken an important step toward realizing the debit routing protections mandated by the existing language in Regulation II but ignored and misconstrued by Visa, Mastercard, and issuers. However, experience has taught us that, unless the Board gives specific and precise guidance on the issues discussed above, its revisions to Regulation II may ultimately amount to naught as they are once again disregarded by these same entities to further their own profits at the expense of merchants and consumers.

Thank you for your consideration of our comments on the Board's proposed revisions.

Sincerely,



Stephanie Martz
Chief Administrative Officer
and General Counsel

[19] *Id.* at 19.