August 10, 2021

By Email to regs.comments@federalreserve.gov

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

Re: Docket No. R-1748, RIN 7100-AG15

Dear Ms. Misback:

The Merchant Advisory Group ("MAG") appreciates the opportunity to comment on the notice of proposed rulemaking issued by the Board of Governors of the Federal Reserve System ("Board") regarding proposed clarifications to Regulation II published in the Federal Register on May 13, 2021. *Debit Card Interchange Fees and Routing*, 86 Fed. Reg. 26,189 (proposed May 13, 2021) ("NPRM"). The MAG's members have suffered acutely from the barriers erected and maintained by networks and issuers to limit merchant routing on all types of debit transactions in ways the Board now recognizes as "inconsistent" with Regulation II. NPRM at 26191-92. These ongoing violations of Regulation II by networks and issuers continue to increase costs to merchants and consumers—by some estimates, by more than $3 billion.[1] The MAG respectfully urges the Board to act as quickly as possible to ensure merchants can route debit transactions as guaranteed by Section 920 of the Electronic Fund Transfer Act ("EFTA") (15 U.S.C. § 1693o–2).

The MAG. Founded in 2008 by a visionary group of merchants dedicated to driving positive change in the payments industry through multi-stakeholder collaboration, the MAG represents more than 165 U.S. merchants in a variety of verticals such as mass merchant, ecommerce, travel and hospitality, quick service restaurants, petroleum, and health care among others, accounting

[1] *See* Meeting Between Staff of the Federal Reserve Board and Representatives of Merchants and Merchant Trade Associations (Sept. 23, 2020), attaching CMSPI presentation titled "Debit Routing in a Changing Retail Payments Landscape" (Sept. 2020) at slide 6 (CMSPI Analysis & Estimates: "Merchant Routing Savings if CNP PINless Was More Prevalent"), https://www.federalreserve.gov/regreform/rr-commpublic/merchants-and-merchant-trade-associations-meeting-20200923.pdf.

for over $4.8 trillion in annual sales at over 580,000 locations across the United States and online. Roughly $3.5 trillion of those sales and over 100 billion card payments are electronic, which represents approximately 62% of total U.S. card volume. [2] MAG members employ over 14 million associates.

I. Introduction

Before addressing the substance of the proposed revisions to Regulation II, the MAG wishes to briefly highlight the history of the market failure in the payments industry that Congress sought to remedy by enacting the Durbin Amendment. That history should guide the Board's approach in this first clarification since the Board's initial rulemaking over a decade ago—especially in light of the president's recent executive order on competition as well as the advances in payments accelerated by the pandemic.

The MAG offers two primary areas of comment for the Board's consideration.

First, the MAG urges the Board to re-examine its decision to interpret the language of Section 920(b) ***not*** to require that issuers enable unaffiliated networks for *each cardholder authentication method that may be used for a debit transaction*. The MAG believes that a requirement for issuers to enable unaffiliated debit routing for all debit transactions, regardless of cardholder verification method, sales channel, type of merchant, or type of transaction, is clear, straightforward, and readily enforced. History demonstrates that the Board's proposed approach requiring routing options for each "type of merchant" and "type of transaction"—while a substantial improvement—may fail in its scope to solve ongoing problems in the routing of debit transactions and may introduce the potential for even greater noncompliance, leaving merchants with only one routing option for many transactions.

Second, the MAG proposes several specific areas for further clarification including, most importantly, the need to directly address routing in the context of tokenized transactions.

II. Background

A. The Durbin Amendment's Routing Provisions Were Enacted to Introduce Competition into a Broken Payments Market

The Durbin Amendment's network routing provisions were enacted in response to the proliferation of exclusive issuance agreements between Visa and Mastercard and debit issuing banks. These agreements eliminated routing competition, resulting in millions of debit cards enabled only for Visa and its affiliated network, Interlink, or Mastercard and its affiliated network, Maestro. The lack of routing competition led to increased interchange and network fees, costing merchants billions of dollars.

Regulation II's routing provisions were designed to fix this problem. As the Board's data has shown for many years, routing competition has worked to reduce interchange fees modestly, as

[2] Source of total U.S. card volumes: *Federal Reserve Payments Study 2019*, https://www.federalreserve.gov/paymentsystems/fr-payments-study.htm.

exempt interchange rates for single-message (generally PIN-authenticated) transactions have fallen nearly to regulated rates, whereas exempt rates for dual-message (generally not PIN-authenticated) transactions have *increased* since 2011.[3] At the same time, despite the elimination of exclusive network agreements, Visa's share of debit volumes has steadily increased since the initial impact from Regulation II, and in 2020 rose to nearly 60%.[4] According to payments industry publication *The Nilson Report*, networks other than Visa and Mastercard comprised just 16.9% of total general purpose debit purchase volume in 2020, down nearly ten percent from 2019.[5] In ecommerce, Visa's debit share is roughly 70%, while Mastercard's share is 25%.[6]

B. COVID-19 Increased Card-Not-Present Transactions and Further Raised Merchant Costs

The Board has identified that issuers and networks have circumvented the routing provisions of Regulation II concerning card-not-present (CNP) transactions. This circumvention has increased costs for merchants. The lack of required routing competition has led to higher exempt interchange rates and network fees for dual-message, card-not-present debit transactions. As volume has shifted to card-not-present transaction types, the problem for merchants grew more severe during the COVID-19 pandemic, as the lack of required routing competition increased payment costs for merchants, and thus their customers, during a time of extraordinary financial stress. As the Board recognized, the already swift growth of card-not-present transactions "accelerated" during the pandemic. NPRM at 26190. These transactions are more expensive for merchants, incurring both higher interchange and network fees. As Board data has shown, where there is routing competition, rates fall; where there is no routing competition, rates increase.

The increase in card-not-present debit stemmed from a massive shift to online shopping, which also was accompanied by a shift toward contactless forms of payment in-store.[7] Retailers

---

[3] *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 3, https://www.federalreserve.gov/paymentsystems/files/debitfees_costs_2019.pdf. As for network fees, the average per-transaction merchant-side network fee paid to dual-message networks "rose consistently from 2009 to 2019 and was the highest average per-transaction network fee across all categories after 2011"—nearly double the fees paid to single-message networks which have "remained constant after 2009 . . . ." *Id.* at 14.

[4] *The Nilson Report* Issues 1005 (Oct. 2012), 1028 (Oct. 2013), 1051 (Oct. 2014), 1074 (Oct. 2015), 1097 (Oct. 2016), 1119 (Oct. 2017), 1141 (Oct. 2018), 1163 (Oct. 2019), 1185 (Oct. 2020), 1191 (Feb. 2021), 1200 (June 2021).

[5] *The Nilson Report* Issues 1185 (Oct. 2020), 1191 (Feb. 2021), 1200 (June 2021).

[6] *See* Complaint, *United States v. Visa Inc. & Plaid Inc.* (N.D. Cal. filed Nov. 5, 2020) ¶¶ 1, 5, https://www.justice.gov/opa/press-release/file/1334726/download ("DOJ Complaint").

[7] *See*, *e.g.*, *Mastercard New Payments Index: Consumer Appetite for Digital Payments Takes Off*, Business Wire (May 4, 2021), https://www.businesswire.com/news/home/20210503005823/en/; Kate Fitzgerald, *Mastercard sees contactless acceptance triple in U.S., Brazil*, American Banker (May 5, 2021), https://www.americanbanker.com/payments/news/mastercard-sees-contactless-acceptance-triple-in-u-s-brazil.

adapted quickly to the pandemic by investing in new forms of shopping such as buy-online-pickup-in-store ("BOPIS") and implementing take-out and delivery in new segments. A senior Visa executive told investors, "we've pulled forward three, four, five years of customer habituation and muscle memory formation" in ecommerce which is unlikely to subside after the pandemic.[8] Meanwhile, debit was already the most popular form of consumer payment for years before the pandemic.[9] The economic disruption wrought by the pandemic increased the use of debit cards, with a shift towards non-discretionary versus discretionary spending, which is disproportionately on debit.

Retailers have operated under tremendous strain over the last 18 months. Some navigated intermittent and unpredictable store closures and lay-offs, while others faced huge spikes in demand offset by persistent supply chain disruptions. Retailers had to quickly learn how to operate during a global health crisis challenging the safety of their employees and customers, with constantly evolving health and safety protocols.[10]

The shift to card-not-present forms of payment has increased costs for merchants, because issuers and networks continue to evade compliance with Regulation II which, as the Board recognized, has resulted in little or no routing choice for this exploding segment of debit transactions. NPRM at 26190 ("merchants are often not able to choose from at least two unaffiliated networks when routing card-not-present transactions"). The MAG urges the Board to end this circumvention without any further delay.

---

[8] Oliver Jenkyn, Executive Vice President & Group President & Regional President-North America, Visa Inc. at Morgan Stanley Technology, Media and Telecom Conference (Corrected Transcript) (Mar. 1, 2021) at 4, https://s1.q4cdn.com/050606653/files/doc_downloads/Transcripts/2020/CORRECTED-TRANSCRIPT-Visa-Inc.(V-US)-Morgan-Stanley-Technology-Media-and-Telecom-Conference-1-March-2021-11-45-AM-ET.pdf); *see also* Visa Inc. at Wells Fargo TMT Summit (Corrected Transcript) (Dec. 1, 2020) at 7 ("[W]e have probably pulled forward three years' worth of behavioral change into one year as a result of the pandemic."), https://s1.q4cdn.com/050606653/files/doc_downloads/events/2020/12/02/CORRECTED-TRANSCRIPT-Visa-Inc.(V-US)-Wells-Fargo-TMT-Summit-1-December-2020-12-00-PM-ET.pdf; Terri Bradford, *Are Contactless Payments Finally Poised for Adoption?*, Federal Reserve Bank of Kansas City, Payments System Research Briefing (Apr. 14, 2021) (discussing the rise in contactless payments and noting surveys indicating that consumers do not expect to revert), https://www.kansascityfed.org/documents/7921/psrb21bradford0414.pdf.

[9] According to the most recent Consumer Payment Choice survey, consistent with prior years, in 2019 "consumers made most of their payments with debit cards . . . ." *2020 Survey of Consumer Payment Choice*, Federal Reserve Bank of Atlanta, Research Data Reports (Updated May 18, 2021), https://www.atlantafed.org/-/media/documents/banking/consumer-payments/survey-of-consumer-payment-choice/2020/2020-survey-of-consumer-payment-choice.pdf.

[10] *See*, *e.g.*, Jason Goldberg, *The Impact Of Covid-19 On U.S. Brands and Retailers*, Forbes (Mar. 29, 2020), https://www.forbes.com/sites/jasongoldberg/2020/03/29/the-impact-of-covid-19-on-us-brands-and-retailers/; Phil Wahba, *A record 12,200 U.S. stores closed in 2020 as e-commerce, pandemic changed retail forever*, Fortune (Jan. 7, 2021), https://fortune.com/2021/01/07/record-store-closings-bankruptcy-2020/.

C. Presidential Executive Order 14036 Makes Vigorous Enforcement of Regulation II an Imperative

On July 9, 2021, President Biden issued an Executive Order on *Promoting Competition in the American Economy*. Executive Order 14036, 86 Fed. Reg. 36,987 (published July 14, 2021). The Order provides valuable context for the Board as it carefully evaluates clarifying Regulation II to better serve the competition-enhancing intent of the Durbin Amendment.

The Order calls for a "whole-of-government approach" to competition policy to combat "excessive market concentration" that threatens to deny American businesses and consumers the benefits of an "open economy." Order at 36987. Section 2(c) of the Order identifies the Dodd-Frank Act specifically as one of several "industry-specific fair competition and anti-monopolization laws" providing "additional protection" above and beyond the nation's antitrust laws, which are the "first line of defense against the monopolization of the American economy." *Id.* at 36989.

Section 2(d) of the Order notes that these statutes charge agencies—including the Board and the Federal Trade Commission ("FTC")—"to protect conditions of fair competition in one or more ways, including by . . . policing unfair, deceptive, and abusive business practices; . . . [and] promulgating rules that promote competition, including the market entry of new competitors . . . ." *Id.* As part of a "whole-of-government approach," Section 2(g) orders that "Agencies can and should further the policies set forth in section 1 of this order by, among other things, adopting pro-competitive regulations . . . ." *Id.* at 36989-90. Finally, in Section 3, the Order encourages renewed inter-agency cooperation where—as here—Congress has adopted laws where "agencies have overlapping jurisdiction." *Id.* at 36990.

The broader failure of market mechanisms in payments led to ever-increasing interchange fees on debit transactions—fees that were as high as those on credit transactions despite the absence of financial risk to the issuer. Additionally, Visa and Mastercard contracted with issuers to be configured as the exclusive network available on issuers' debit cards, leveraging their power in credit to advance their fraud-prone signature debit products and diminish rival debit networks who offered more secure PIN transactions.

These developments led to the Durbin Amendment. Enacted as part of the Dodd-Frank Wall Street Reform and Consumer Protection Act in 2010, the Durbin Amendment sought to bring about competition and transparency into debit transactions by regulating interchange fees for covered issuers (issuers with $10 billion or more in assets) and requiring two unaffiliated networks on all debit products to allow for merchant routing choice.[11]

The Department of Justice ("DOJ"), in carrying out its mission as one of the two federal agencies charged with enforcing the antitrust laws, recently recognized these debit market realities (and Regulation II's inability to remedy them) when it sued to block Visa's acquisition of Plaid under Section 2 of the Sherman Act and Section 7 of the Clayton Act in *United States v. Visa Inc. &*

[11] *See* Section 1075 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Pub. L. 111–203, 124 Stat. 1376 (2010)), which amended the EFTA (15 U.S.C. § 1693 et seq.) by adding a new Section 920 codified at 15 U.S.C. § 1693o–2.

Plaid Inc. (N.D. Cal. filed Nov. 5, 2020) ("DOJ Complaint"). The DOJ Complaint alleged that Visa continues to possess and wield monopoly power in the debit market, citing the high "entry barriers, coupled with Visa's long-term, restrictive contracts with banks" as "nearly insurmountable" to competitors. DOJ Complaint ¶ 6. The DOJ further alleged that Visa has maintained that power by, among other things, subverting the successful implementation of the Durbin Amendment. *Id.* ¶ 31 ("Visa has responded by imposing new fees on merchants that undermine the effectiveness of the Durbin Amendment's fee caps. Even after enactment of the Durbin Amendment, Visa estimates that it earns an 88% operating margin from its network fees on debit payments, illustrating its durable monopoly power."). According to the DOJ, "the debit network and interchange fees that Visa and its partner banks collect cost U.S. merchants and consumers more than $6 billion per year." *Id.* ¶ 28. At the same time, the MAG is aware that Mastercard—"Visa's only meaningful competitor for card issuance," *id.* ¶ 27—has made similar agreements with issuers where Mastercard must be the only signature network enabled on Mastercard-branded debit cards, further restricting merchant routing options for card-not-present transactions.

The market failure identified by the DOJ requires constant and rigorous enforcement of the Durbin Amendment. Over the years, issuers and networks have consistently worked to erode the two pillars of the Durbin Amendment—a cap on the level of interchange fees and a ban on network exclusivity. The history of circumvention by issuers and networks is starkly evident in the Board's recent data showing "covered issuers representing slightly more than 50 percent of the total number and value of all covered transactions reported that *none of their CNP transactions were processed over single-message networks in 2019*."[12] We laud the Board's attention to this problem and now turn to the specific clarification proposed in the NPRM.

III. The Board Should Require Routing Options for All Methods of Cardholder Authentication, Regardless of Means of Access

The MAG appreciates that the Board makes clear in its proposed revisions to Official Commentary to Section 235.7 that Regulation II's network non-exclusivity provisions require that a debit card be enabled on at least two unaffiliated payment card networks "regardless of means of access," including explicitly any "means of access that may be developed in the future." NPRM at 26195 (Proposed Comment 235.7(a)-(7)).

However, the MAG is concerned that the Board intends to maintain its earlier position[13] that there is no requirement that an issuer enable two unaffiliated networks for "each method of cardholder authentication (*e.g.*, signature, PIN, biometrics, any other method of cardholder

[12] *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 17, https://www.federalreserve.gov/paymentsystems/files/debitfees_costs_2019.pdf.

[13] The MAG observes that while the Board previously defended its position on routing and authentication methods in litigation, the D.C. Circuit affirmed that the Board retains discretion under the statute. *NACS v. Board of Governors of the Federal Reserve System*, 746 F.3d 474, 493-96 (D.C. Circ. 2014) ("defer[ing] to the Board's reasonable interpretation of section 920(b)").

authentication that may be developed in the future, or the lack of a method of cardholder authentication)." NPRM at 26194 (Proposed Comment 235.7(a)-(1)).[14]

Allowing issuers not to properly enable two unaffiliated networks for each method of cardholder authentication risks perpetuating the problems that motivated the Board's clarification in the first place. Issuers' failure to enable routing options for all cardholder authentication methods has resulted in issuers denying merchants the ability to route transactions on card-not-present transactions for many years, including by actively disabling certain cardholder verification methods ("CVMs") supported by unaffiliated networks. Networks and issuers that wish to continue to circumvent the Board's clarified rule may even assert that routing need not be enabled for certain card-not-present transactions, depending on what methods are used to authenticate the cardholder. Those that wish to continue to circumvent Regulation II may simply engage third parties to deploy technology to authenticate the cardholder and claim that it is the third-party's technology that bars routing, not the issuer.

The Board's approach may also fail to address current circumvention efforts that often eliminate PINless routing options for *card-present* transactions, or it may introduce additional means of evasion of the Board's routing requirements.[15] If customer "muscle memory" learned during the pandemic leads to lower PIN entry, it is all the more important to have at least two unaffiliated routing options available for CVMs that do not use PIN, such as No-CVM, biometric, or signature transactions.

Specifically, the MAG is concerned that issuers could deploy a patchwork of enablement of unaffiliated networks for certain *types* of transactions, but *for only certain authentication methods*. For example, in the card-present context, even though networks finally eliminated signature-capture requirements, if issuers do not enable PINless functionality, merchants will only have routing options when a PIN is obtained. Networks and issuers could further limit the number of transactions with multiple routing options— "contestable" transactions, in industry parlance—by only enabling routing options when authentication methods that are less prevalent than PIN are used, such as a biometric method, while enabling only a single network for more established methods. Networks and issuers could then claim they are still in compliance with Regulation II by using this authentication loophole. It is exactly this type of conduct—where issuers and networks find ways to effectively evade compliance with Regulation II—that led to

[14] As the Board is aware, the non-exclusivity mandate in the statute bars restrictions on the routing of a debit "transaction." 15 U.S.C. § 1693o-2(b)(1)(A) & (B). The provision's author, Senator Durbin, confirmed on the Senate floor during debate on this legislation that "[t]his paragraph is intended to enable each and every debit card transaction—no matter whether that transaction is authorized by a signature, PIN, or otherwise—to be run over at least two unaffiliated networks." Cong Rec. S. 5926 (July 15, 2010). Through its Frequently Asked Questions ("FAQs"), the Board at other times has indicated that routing limitations may not be imposed based on cardholder authentication methods. *Frequently Asked Questions About Regulation II (Debit Card Interchange Fees and Routing)* on § 235.7 Network Exclusivity and Routing Provisions (Last Update: Nov. 2, 2016) at Q1, Q3, Q4, https://www.federalreserve.gov/paymentsystems/regii-faqs.htm.

[15] As discussed below, the Board should expressly clarify that "low-value transactions" and automated fuel dispensers ("AFDs") are respectively a "particular type of transaction" and "particular type of merchant" where issuers must enable routing to unaffiliated networks.

this proceeding. In short, cardholder authentication methods should not be used to continue to manufacture and exploit routing obstacles.

To avoid these problems, the Board should require unaffiliated networks be enabled for every method of cardholder authentication. This could be accomplished by requiring that if an issuer enables a network, it must enable that network for all methods of cardholder authentication that the network supports.[16] In addition, no network should be able to restrict or interfere with another network's access to any cardholder verification method.[17]

The Board can accomplish this clarification by expanding the current proposed language concerning non-exclusivity for every "particular type of transaction" (in Section 235.7(a)(2) and in Proposed Comment 235.7(a)–(2)(iii)(B)),[18] to apply regardless of the method of cardholder authentication. This clarification would avoid any ambiguity about whether a particular transaction is a discrete *type* of transaction—*e.g.*, card-present—or uses a discrete *method of authentication*, such as biometric. The MAG proposes that the Board modify the proposed language "for every . . . particular type of transaction" to be more inclusive of new transaction types by including the following language: "for every particular type of debit transaction, regardless of cardholder authentication (*e.g.*, signature, PIN, biometrics, any other method of cardholder authentication that may be developed in the future, or the lack of a method of cardholder authentication)."

In the past, networks and issuers have argued that adding additional networks for dual-message transactions would be costly, and that cardholders preferred one network over another and therefore needed to be able to select which network routed their transaction. Even today, Visa rules bar merchants from requiring PIN entry, which Visa has justified on the basis of cardholder choice of network. In November 2016, however, the Board emphasized that Regulation II provides routing choice to *merchants*.[19] The additional-cost argument is belied by the fact that issuers have actively *disabled* PINless functionality otherwise ready and available from unaffiliated networks, in order to reduce competition and maximize their own profitability via volume incentive agreements.

Some have suggested that PINless routing has not been widely deployed because it is new and unproven. However, unaffiliated networks have supported PINless routing for years and issuers

---

[16] The Board could also clarify that while an issuer should enable all the cardholder authentication methods supported by a given payment network, it is under no obligation to enable such methods if they are not properly supported. Genuinely innovative authentication methods could be deployed even if only supported by a single network; however, when other networks develop support for these methods, issuers should be required to enable these networks to allow merchant routing.

[17] Since 2014, Visa and Mastercard have agreed to license only PIN CVM and No-CVM functionality on EMV chip cards for unaffiliated networks, restricting access to signature CVM and CD-CVM, which includes biometric authentication. This is an example of routing interference that should be prohibited.

[18] NPRM at 26192, 26194.

[19] *Frequently Asked Questions About Regulation II (Debit Card Interchange Fees and Routing)* on § 235.7 Network Exclusivity and Routing Provisions (Last Update: Nov. 2, 2016) at Q4, https://www.federalreserve.gov/paymentsystems/regii-faqs.htm.

have taken *affirmative steps* to disable PINless functionality for certain transaction sets. Unaffiliated networks with longstanding PINless capability include STAR ACCESS (STAR network), ANP+ (ACCEL network), PULSE PAY Express (PULSE network), Sure Pass and Elite Pass (SHAZAM network), and NYCE PINless POS (NYCE network). The restrictions on routing that the Board identifies in the NPRM are not the result of technical limitations; they are the result of business rules put in place by issuers because of incentives from the dominant networks.

As for cardholders, in the MAG's experience, consumers are generally indifferent to how their transactions are routed. Issuers apply consistent liability policies across all the networks they enable for their cardholders, and networks likewise maintain consistent zero liability policies. The dominant networks have also suggested that PINless transactions represent a fraud risk. This argument has no support—unaffiliated networks deploy robust fraud prevention technology, as do issuers as part of their authorization routines. Existing data also refute the argument—overall, dual-message transactions suffer three times the rate of fraud loss as single-message transactions. While fraud rates are based on lower volumes because of the circumvention at issue here, to date the fraud rate on single-message card-not-present transactions is substantially lower than for dual-message transactions.[20]

IV. The Board Should Clarify That Tokenized Transactions Must Be Fully Routable

The MAG supports the Board's efforts to clarify that debit card issuers must properly enable, and allow merchants to choose from, at least two unaffiliated networks for all types of transactions. Considering the history of circumvention of Regulation II by issuers and networks, the MAG urges the Board to make additional efforts to ensure compliance in the future.

The MAG also supports the Board's clarification that a debit card must be enabled for at least two unaffiliated payment card networks "regardless of means of access," including explicitly any "means of access that may be developed in the future." NPRM at 26195 (Proposed Comment 235.7(a)-(7)). Additionally, the MAG supports the Board's proposed commentary that such means of access include a debit card as well as card proxies such as a device like a fob, or "information stored inside an e-wallet on a mobile phone or other device." *Id.* The proposed commentary properly requires that for any means of access that carries debit information—whether a card or other device—two unaffiliated payment networks must be enabled by the issuer.

The MAG encourages the Board to be clearer still in its commentary, bearing in mind the history of market failure and regulatory whack-a-mole in the payments industry leading to this very proceeding. Today, there are many solutions in market that allow merchants to access customer debit cards stored "on file" or in e-wallets for consumers to make in-app purchases. However, these solutions are routinely structured by issuers and networks to effectively deny merchants the ability to route to unaffiliated networks. The MAG believes it is important to clarify that debit

[20] *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 17, https://www.federalreserve.gov/paymentsystems/files/debitfees_costs_2019.pdf.

transactions conducted in-app or by using a card stored on file are fully "card-not present transactions," a "type of transaction" for which at least two unaffiliated networks must be enabled and available.[21] The MAG highlights that these are fast-growing and increasingly common use cases, such as where a customer has stored payment credentials on a merchant website for subsequent purchases or recurrent billing—from Uber to Netflix to Spotify to various buy-online-pickup-in-store or delivery solutions.

The MAG also believes it is critical for the Board to understand that security methods such as tokenization, in particular, is a continuing and growing area where issuers and networks inhibit merchant routing to unaffiliated networks. The DOJ acknowledged the impediments created by Visa when challenging Visa's merger with Plaid:

> These smaller PIN networks, such as Accel, Star, NYCE, and Pulse, have some meaningful presence for in-person debit transactions, but have yet to overcome the barriers to entry for online transactions. ***This is in part because Visa has erected technological barriers (such as Visa's tokenization service, which withholds essential data from PIN networks) and entered into restrictive agreements that disincentivize the use of PIN networks.*** As a result, merchants do not use PIN networks in any significant volume to process online transactions, and instead pay higher fees to use Visa and Mastercard networks. [22]

Tokenization is the process of protecting sensitive data by replacing it with an algorithmically generated number called a token. In payment card tokenization, the customer's primary account number ("PAN") is replaced with a series of randomly generated numbers, called a "token." Tokens can be passed throughout the payment chain without exposing sensitive banking details. Visa and Mastercard network tokens have been increasingly used in digital wallets such as Apple Pay and Google Pay.

While tokens themselves are good for the ecosystem, the way they are required to be treated by the creator of the token can reduce routing options. For instance, by agreement between issuers and Visa and Mastercard (and without any involvement from merchants), tokens that are created by Visa and Mastercard must be sent back to these networks for the actual PAN to be regenerated for the issuer to approve the transaction. This creates a technical barrier in the routing of transactions and leaves the global network as the decider of whether the transaction is routable and what information from the original transaction will be included if it is routable.

To provide a minimal level of compliance with Regulation II in the case of digital wallets used at the point-of-sale, Visa and Mastercard have provided a "call-out" service to detokenize the transaction and provide the PAN to enable routing over unaffiliated networks, which permits the merchant a measure of routing choice when a customer accesses a debit card stored on a mobile

---

[21] Alternatively, the Board could recognize "in-app" transactions on mobile devices as a discrete type of transaction, rather than parsing whether these are card-present (such as when the same device interacts with a terminal via Near-Field Communication ("NFC"), without a physical card) or card-not-present transactions.

[22] DOJ Complaint ¶ 32 (emphasis added).

device. The MAG understands that Visa and Mastercard provide this call-out service when a cardholder is using a mobile device at the physical point-of-sale. When the cardholder is accessing the same information stored in a mobile wallet through an application on the phone, or a website, however, no call-out is generally provided and routing choice required by the law is rendered impossible.

Visa has modified its position on this call-out in response to merchant complaints, while Mastercard has refused to do so.[23] But despite its modified position, Visa strips critical data elements—including cryptogram validation and domain channel information—out of the transaction, preventing the issuer from authenticating the token, authenticating the merchant, and authorizing the transaction. Importantly, Visa provides these necessary details to unaffiliated networks when the cardholder is present in-store; it is only on in-app or online, card-not-present transactions where this essential data is stripped.[24] And of course, Visa provides these details to the issuer for all of its *own* transactions. At the same time, Mastercard refuses to detokenize card-not-present transactions *at all*.

Proposed Clarification. The MAG proposes that the Board adopt language further clarifying that implementation of security solutions, like tokenization, for debit card transactions may not come at the cost of inhibiting routing options directly (by mandating exclusive use of tokens) or indirectly (by withholding relevant and critical data elements). The Board can accomplish this goal by adopting a standard that requires that, when network tokens are deployed, minimal compliance via a call-out to provide the PAN is necessary but is not sufficient, and instead all information needed to consummate the transaction must be provided on a non-discriminatory basis.

Similarly, networks should be prohibited from requiring the provision of data *to the network-token-provider* concerning the transaction, other than what is necessary to detokenize. The MAG understands that both Visa and Mastercard have required the unaffiliated network and/or the merchant to provide additional data—including competitively sensitive data—about transactions routed to unaffiliated networks. To be clear, these requirements mean that merchant data is shared *with a network that is not even processing the transaction*.

Another way to rectify this problem would be to require that all forms of account numbers rendered to the merchant must be able to be sent directly to the issuer. This would put the onus on the issuer to seek any additional information needed to approve the transaction instead of the merchant or acquirer. Here, the token-service-provider ("TSP") would share the necessary

---

[23] The MAG understands that Mastercard also imposes a fee on issuers for all volume processed on non-Mastercard networks. This fee, called the Domestic Other Non-MasterCard Processed Purchase Volume Fee, assesses a charge of 3 basis points when a purchase initiated with a Mastercard-branded card is transacted over another card network that is also enabled on the card, even though Mastercard provides no services at all on the particular transaction.

[24] Visa and Mastercard have long agreed to fully detokenize *each other's* transactions, since 2016. *Mastercard And Visa Tag-Team Tokens*, PYMNTS (Dec. 16, 2016), https://www.pymnts.com/news/mobile-payments/2016/mastercard-and-visa-tag-team-tokens/; *Visa expands secure digital payments in Visa Checkout through tokenization agreement*, Visa.com, https://usa.visa.com/visa-everywhere/security/secure-digital-payments-through-tokenization.html.

information with the issuer in advance, which would allow the issuer to detokenize the transaction. Similarly, another alternative would be to prohibit a network-specific token and to require a network-agnostic token, which would be generated with the issuer owning the algorithm to decode the transaction.

As tokenization is increasingly used throughout the payment ecosystem, it is imperative that the Board make clear that debit card issuers must properly enable, and allow merchants to choose from, at least two unaffiliated networks for all types of transactions, without using tokenization as a technical barrier to prevent routing.

V. Small-Ticket and AFD Transactions Are Discrete Card-Present Merchant Transaction Types

The MAG requests that the Board clarify that, like card-not-present transactions, small-ticket or "low-value" transactions are considered "a particular type of transaction for which two unaffiliated payment card networks must be available." NPRM at 26190, 26192. The NPRM references "low-value card-present transactions" as a growing area and presumably references these transactions in Proposed Comment 235.7(a)–(2)(iii)'s example of a specific type of merchant, a "fast food restaurant." NPRM at 26191 n.17, 26194.

Similarly, the Board should further clarify that automated fuel dispenser ("AFD") transactions are transactions of a "particular type of merchant" for which routing must be enabled. Both transaction sets have seen problems with PINless enablement in the market, likely due to issuers disabling unaffiliated networks on these types of transactions pursuant to incentive agreements with Visa or Mastercard.

To remove any conceivable doubt about the application of Regulation II to these merchants and these transactions, the MAG suggests the following revision to Proposed Comment 235.7(a)-(2)(iii), underlined in red:

> iii. *Examples of permitted arrangements*. For every geographic area (*e.g.*, New York State), specific merchant (*e.g.*, a specific fast food restaurant chain), particular type of merchant (*e.g.*, fast food restaurants, automated fuel dispensers), and particular type of transaction (*e.g.*, card-not-present transaction, low-value transaction) for which the issuer's debit card can be used to process an electronic debit transaction, an issuer must enable at least two unaffiliated payment card networks, but those payment card networks do not necessarily have to be the same two payment card networks for every transaction.

VI. Use of Proprietary Specifications to Create Barriers to Routing

The global networks continue to leverage EMVCo and its limited ownership structure to create specifications that in turn limit routing capabilities. Within EMVCo, unaffiliated networks are relegated to the role of technical advisors. The implementation of EMV 3-D Secure (EMV 3DS) is an example. Here, EMVCo has adopted a specification that may be used to authenticate a cardholder in ecommerce for participating issuers. The specification allows for rules that make routing of debit transactions impossible, thus not complying with the law, as well as permitting the imposition of additional fees.

Similarly, the global networks recently agreed to drop their competing "buy buttons" such as Masterpass and Visa Checkout (which saw little merchant adoption). Through an EMVCo standard, these networks have instead combined to introduce a single button for ecommerce purchases. In late 2019, this solution was re-branded "Click to Pay." The product is clearly an attempt by Visa and Mastercard to band together to compete against PayPal,[25] which has wide adoption by merchants and consumers. Yet the Click to Pay product—in which all issuers automatically participate—is based on the EMVCo SRC specification that allows for rules that make routing of debit transactions impossible. As noted above in the discussion of the use of authentication methods to create a routing loophole, if as some networks have suggested, Click to Pay is considered a method of cardholder authentication, networks and issuers will act as if these transactions (which rely on network tokens) need not be routable.

The Board should further clarify that the use of standards such as 3DS, QR codes, or for products such as Click to Pay, should not require merchants to surrender routing rights. It is essential to future-proof Regulation II so that the inevitable implementation of new standards or technological enhancements by networks, issuers, or their agents throughout the payment ecosystem, do not eliminate merchant routing options. The MAG would welcome regular, effective enforcement of Regulation II given the dynamic and changing nature of the payments marketplace and its technology, and the history of effective evasion of regulation by the networks and issuers.

VII. Ensuring the Price of Regulated Transactions Are Proportional to Issuer Costs

The Board appreciates that while the NPRM does not directly address interchange fees for covered transactions, "[t]he Board will continue to review the regulation in light of the most recent data collected by the Board pursuant to EFTA section 920 and may propose additional revisions in the future." NPRM at 26190.[26]

The MAG urges that the Board undertake this review and reduce regulated debit interchange fees as soon as possible. The data most recently collected by the Board observed issuer costs "nearly halving" to less than 4 cents per transaction.[27] Yet, the Board has made no adjustments to the regulated rates. At the same time, the Board notes that "[t]he share of fraud losses absorbed by

---

[25] *See* DOJ Complaint ¶ 46 (detailing Visa's "long history of protecting its monopoly in online debit by entering into contracts that forestall entry and coopt would-be rivals" like PayPal).

[26] Merchants and their representatives submitted detailed data on this issue to the Board last year. *See* Meeting Between Staff of the Federal Reserve Board and Representatives of Merchants and Merchant Trade Associations (Sept. 23, 2020), attaching Letter to Federal Reserve Chairman and Governors (July 27, 2020), https://www.federalreserve.gov/regreform/rr-commpublic/merchants-and-merchant-trade-associations-meeting-20200923.pdf.

[27] *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.

issuers and merchants changed significantly from 2011 to 2019, with issuers absorbing a smaller share and merchants absorbing a larger share across all transaction categories and fraud types."[28]

This data means that, contrary to the EFTA, interchange fees are currently not "reasonable and proportional to the cost incurred by the issuer with respect to the transaction." 15 U.S.C. § 1693o–2(a)(2)-(3). The Board should lower the regulated rate (and eliminate the ad valorem fraud reimbursement) based on this latest cost survey, because current rates are no longer "reasonable and proportional" as issuer costs continue to decline and merchant fraud losses continue to increase.

The MAG also observes that, even though costs for issuers have declined, the regulated rate has become a floor and there is no competition below the cap. The MAG requests that the Board monitor and investigate the reasons why (1) debit interchange fees for regulated issuers have not been competed below the cap; and (2) debit interchange fees for dual-message transactions on unregulated issuers' cards have remained significantly higher than all other debit transactions.

Finally, the MAG believes that the Board should revisit the continuing necessity to allow issuers, with minimal certification of their efforts, to collect a penny per transaction for the fraud prevention adjustment. Merchants have spent billions in infrastructure investments since 2012 to enable EMV-compliant terminals, and many incurred millions in EMV chargebacks through no fault of their own because Visa and Mastercard caused delays in the development of EMV chip debit routing specifications.[29] In fact, merchants incurred the vast majority of the expenditure required to migrate the U.S. payment system to the more secure EMV technology. Merchants also continue to invest heavily in the security of their customers' ecommerce purchases. As the Board's data shows that merchants (and consumers) bear an increasing majority share of all fraud losses, this fraud prevention adjustment is no longer necessary or appropriate, and should be eliminated.

VIII. Other Areas of Continued Monitoring, Investigation and Potential Rulemaking

The Board has indicated that it will continue to review the regulation and may propose additional revisions in the future. The MAG welcomes this initiative—which is especially appropriate in light of the Executive Order—and believes it should be conducted without delaying the implementation of the currently proposed changes or enforcement of the law.

The MAG urges the Board to vigilantly focus on areas of violations or circumvention in all environments (card-present or card-not-present) and ensure that there are strict timelines to restore problems that are identified. Without such strict timelines, changes are slow, and the long-term effects of circumvention efforts continue to be felt in the market.

---

[28] *Id.* at 19 & Fig. 17.

[29] Fumiko Hayashi, Zach Markiewicz and Sabrina Minhas, *The Initial Effects of EMV Migration on Chargebacks in the United States*, Federal Reserve Bank of Kansas City (Dec. 2018) at 7 (Federal Reserve working paper noting that "variation in the liability shift across networks made EMV adoption more complex"), https://www.kansascityfed.org/~/media/files/publicat/reswkpap/pdf/rwp18-10.pdf.

The U.S. migration to EMV chip technology is one such example. Visa and Mastercard delayed bringing chip technology to the U.S. despite rising domestic fraud and fraud migration to the U.S. for many years to protect their lucrative, but fraud-prone signature debit products, leaving the U.S. as the last country in the world to migrate to chip.[30] After Regulation II reduced signature debit interchange to the same level as PIN debit for covered issuers, Visa and Mastercard introduced EMV chip technology only because signature debit's high fraud rates were unsustainable and Visa and Mastercard controlled the technology and could use it to subvert Regulation II. These networks then adopted rules to prohibit routing from their proprietary chip technology widely used across the globe, forcing U.S. industry stakeholders to agree to share sharply limited access to their EMV applications, which led to an unnecessarily complex EMV implementation in the U.S. This bifurcated access to widely used chip technology—with one "global" AID and one "common" AID—complicated routing and provided only limited access to CVMs, as only PIN and No-CVM were made available to unaffiliated domestic networks. The global networks thus introduced routing impediments through EMV, despite the fact that routing from chip cards is no different than routing from magnetic stripe cards—it is accomplished by the use of BIN tables. This strategy resulted in a complex dual-AID implementation in the U.S. unlike any other in the world, including countries where there is also more than one debit network enabled on cards.

The impact of this conduct is still evident today, as we continue to see in the market "US Debit/Visa Debit" point-of-sale screens which reflect the dual-AID infrastructure in the U.S. developed in response to Visa's rules about securing 'cardholder choice.' Nearly five years later, these screens persist after the Board FAQ intended to address them and after Visa's agreement with the FTC to drop this aspect of its Honor All Cards rule and related implementation guides. Those screens confused consumers into making Visa Debit transactions rather than PIN transactions on unaffiliated networks, reinforcing Visa's monopoly power, and their effect can still be seen today.

The MAG appreciates the Board's continued efforts and remains available to discuss its comments and future areas of inquiry.

Respectfully,

John Drechny
CEO
Merchant Advisory Group

---

[30] *See, e.g.*, Richard J. Sullivan, *Can Smart Cards Reduce Payments Fraud and Identity Theft?*, Federal Reserve Bank of Kansas City, Economic Review (3d Quarter 2008) at 51 (citing one "challenge" impeding the U.S. market's migration to EMV that "[B]anks make more revenue from signature debit compared to PIN debit. *Because the EMV and [other chip card] standards would essentially eliminate signature debit, bank revenue for payment services could be reduced.*") (emphasis added), https://kansascityfed.org/documents/1114/2008-Can%20Smart%20Cards%20Reduce%20Payments%20Fraud%20and%20Identity%20Theft%3F.pdf.