February 13, 2023

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC-5610 (Annex Q)
Washington, DC 20580

RE: Mastercard Incorporated; File No. 201 0011

Dear Sir or Madam,

The Merchants Payments Coalition (MPC)[1] appreciates this opportunity to provide comments on the recently announced proposed settlement between the Federal Trade Commission (FTC) and Mastercard, Inc. relating to Mastercard's tokenization policies and violations of Federal Reserve Regulation II.

Competition in the payments ecosystem is important for merchants, their employees, consumers, and the economy at large. We appreciate the work of the FTC to investigate these issues and seek reform of Mastercard's practices. This is a market that is easy to ignore because consumers do not see the fees that are imposed on merchants when accepting debit cards. But, debit and credit card fees are, on average, merchants' second-highest operating expense (behind labor) and reached nearly $140 billion in 2021 alone. And, as the FTC acknowledges, while these fees are paid directly by merchants, they are ultimately borne by consumers.[2] The FTC's efforts in this area, then, are valuable in bringing attention to the regulatory and competition policy violations of Mastercard's actions.

We do, however, have concerns about the proposed settlement and believe more must be done to ensure that the debit market benefits from competition in a manner required by Regulation II. We hope that these comments will provide a path for the FTC to revise the proposed settlement before it is finalized.

Just as our own members compete against each other for business, with competition driving down prices and increasing quality, we are 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

[1] The Merchants Payments Coalition is a group of retailers, supermarkets, restaurants, drug stores, convenience stores, gas stations, online merchants, and other businesses focused on reforming the U.S. payments system to make it more transparent and competitive. MPC firmly believes in opening up the payments market and introducing competition, which in turn would lower costs and drive innovation. Additional information on the MPC can be found at https://merchantspaymentscoalition.com/.

[2] FTC Draft Complaint, *In the Matter of Mastercard* ("Draft Complaint"), para. 4.

competition has been elusive as Visa and Mastercard (the "Global Networks"), the dominant networks in both credit and debit, time and again have taken aggressive action to ensure that any opportunity for competition has been quashed.

The Continuing Attacks on Merchant Routing Choice for Card Not Present Transactions

When promulgated, Regulation II was intended to introduce competition into the otherwise noncompetitive—or anticompetitive—debit market. Among other things, Regulation II implemented two critical requirements with respect to debit routing. First, each issuer was required to enable at least two unaffiliated debit networks on each of its debit cards. Second, issuers and networks were precluded from inhibiting merchants from routing debit transactions over either of the networks for which a card was enabled. In theory, particularly as other networks 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 (CNP) transactions[3]—merchants should today have at least two debit networks available for virtually every one of their debit transactions. But that has not transpired. In particular, merchants' ability to route CNP transactions over any network other than the Global Networks remains severely curtailed as a result of the Global Networks blocking (or incentivizing debit card issuers to block) these transactions from being processed by the competitive networks. This necessitated the Federal Reserve to act last year, clarifying that the routing protections of Regulation II apply not only to card present (CP) transactions, where the card is physically present at the time of purchase, but equally to CNP transactions.

There are two primary reasons the Global Networks have focused—and continue to focus—on CNP transactions in their anticompetitive attacks on debit routing choice. First, prior to enactment of Regulation II and the competitive networks' development of the ability to process CNP transactions, the Global Networks each had monopolies over these transactions.[4] The status quo was threatened by Regulation II, and the Global Networks have always been willing to fight fiercely to defend their profitable monopolies.

Second, CNP transactions reflect a significant *and growing* portion of the payments accepted by merchants. As stated in an industry study cited on the Mastercard website, *card-not-present transactions grew by 23% in 2020 alone*[5]—a year in which overall transactions fell by 2.5% due to the pandemic.[6] As the FTC notes in its Draft Complaint, "[T]he volume of debit card purchases made online rather than in stores has grown significantly in recent years, a trend accelerated by the COVID-19 pandemic."[7] And this growth is not fleeting, as it continues even

[3] CNP transactions include all e-commerce transactions such as purchases made on a personal computer or on a browser or app on the cardholder's phone, together with mail order/telephone orders, recurring billings, and any other transaction in which the cardholder does not present a physical card at the point-of-sale.
[4] Thus, for example, when a cardholder made a CNP purchase using a debit card enabled for the Mastercard network, the merchant had no choice other than to route the transaction over Mastercard. This gave Mastercard a monopoly over all CNP transactions conducted with that card.
[5] https://www.mastercard.com/gateway/vision/insights/improving-cnp-approval-rates.html, citing "2021 Debit Issuer Study: Debit's Transformation Accelerates" (https://content.pulsenetwork.com/debit-issuer-study/2021-debit-issuer-study-white-paper#main-content).
[6] 2021 Debit Issuer Study: Debit's Transformation Accelerates, p. 2.
[7] Draft Complaint, para. 3. *See, also, id.* at para. 23 ("Ecommerce debit transactions have come to represent an increasingly important share of the debit landscape. Analyses by the Federal Reserve Board report a marked increase

as the impact of the pandemic lessens. As one debit card issuer in the study cited by Mastercard states: "Trends we thought would play out over five years accelerated into one year. Card-not-present behavior is here to stay, and we think it will grow even more."[8]

As discussed below, the most recent attack by the Global Networks on CNP transactions has focused on tokenized CNP transactions. The number of tokenized transactions—including transactions conducted using e-wallets—has also continued to grow exponentially. As the FTC notes, "[o]nline growth has been particularly rapid for debit cards used in ewallets such as Apple Pay, Google Pay, and Samsung Wallet. Ewallets from these and other providers offer consumers convenience and security benefits and have become increasingly popular."[9] According to the study cited on Mastercard's website, the majority of e-wallet transactions are in-app purchases—a type of CNP transaction.[10] According to a recent industry study, "the total number of tokenized payment transactions will exceed 1 trillion globally by 2026; rising from 680 billion in 2022. This represents a growth of 58% over the next 4 years."[11]

Clearly, any restrictions on the ability of merchants to route transactions that fall under both of these growing categories—*CNP transactions* that are *tokenized*—is of great significance to merchants. It is also, of course, of great import to the Global Networks as their ability to maintain routing control over these growing categories of transactions increases the amount of money flowing from merchants' pockets into their own. It is for this reason that they have targeted *card-not-present tokenized* transactions for special treatment. This is, no doubt, a daring move given the Federal Reserve's recent efforts to ensure that CNP and CP transactions are treated on equal footing. And it is one that the FTC should quash.

Mastercard's Inhibition of Card Not Present Tokenized Transaction Routing

The 16-digit number that ordinarily appears on a cardholder's debit card is known as the Primary Account Number (PAN). Tokenization is a process through which this number 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. The MPC and its members strongly support tokenization as a security measure. But, unfortunately, the process has been weaponized by Mastercard (and Visa) as a means of preventing competition from the competitive networks.

To understand the problem, it helps to recognize how tokenization works in today's payments system. Mastercard offers tokenization services through which, at the request of a card issuer, it translates the issuer's PANs into tokens. Once it assigns a token to a PAN, it lists both the PAN and its assigned token in a look-up table which allows it to translate the token back into a PAN. Since only Mastercard knows which tokens relate to which PANs, no one but Mastercard is able

in the volume of ecommerce transactions since 2012, and the shift from in-person to ecommerce transactions accelerated during the COVID-19 pandemic.")

[8] 2021 Debit Issuer Study: Debit's Transformation Accelerates, p. 1.

[9] Draft Complaint, para. 3.

[10] 2021 Debit Issuer Study: Debit's Transformation Accelerates, p. 3 ("Most mobile wallet transactions (57%) are made in-app, with the rest being in-store.").

[11] Juniper Research, "Payment Tokenisation: Key Opportunities, Segment Analysis & Market Forecasts 2022-2027," https://www.juniperresearch.com/pressreleases/tokenised-payment-transactions-to-exceed-1tn.

to detokenize the token back into a PAN. Every debit card issuer in the United States that issues debit cards enabled for the Mastercard network uses Mastercard to tokenize its debit cards. Thus, for example, if a cardholder seeks to load 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 Mastercard at the issuer's request. When that token is then presented to a merchant, there is no way for the merchant to determine the original PAN, and the transaction cannot be processed until it is detokenized back into a PAN by Mastercard. In addition to translating the token back into a PAN, the detokenization process also includes the application of several security protections intended to ensure that the token is not being used in a fraudulent manner. This is done through processes known as cryptogram authentication and domain restriction validation.

If the merchant chooses to route a tokenized transaction over the Mastercard network, Mastercard—since it originally provisioned the token—has the data necessary to detokenize it and apply the two validation checks as part of the ordinary transaction flow. But only Mastercard, as the entity that provisioned the token, has access to this data. Therefore, if the merchant instead seeks to route a debit transaction over the competitive network for which the card is enabled, that network cannot process the transaction without including Mastercard in the transaction flow. Mastercard therefore can block any transactions on the card from being processed over any network other than Mastercard. And Mastercard has done exactly this.

Specifically, Mastercard has been arbitrarily selective about whether it is willing to detokenize the PAN, based on whether the transaction is a CP or CNP transaction. If the transaction is a CP transaction, Mastercard is willing not only to detokenize the PAN, but also to validate the cryptogram and domain restrictions. But if it is a CNP transaction, Mastercard refuses to detokenize the transaction outright, taking away the merchant's routing choice. By virtue of Mastercard's refusal, these transactions are only routable to Mastercard. It is notable that Mastercard acts this way *only* when the merchant attempts to route a CNP transaction to a competitive network. As with Mastercard's other conduct, the focus of its policies is protecting its grip on CNP transactions. As the FTC aptly explains in describing Mastercard's policy:

> Mastercard's token policy reflects a business decision to protect and increase Mastercard's debit revenue, as opposed to any technical limitation on Mastercard's ability to allow merchant routing choice for card-not-present ewallet transactions.[12]

This is of great significance to merchants, as every token that is provisioned for a debit card that is enabled for the Mastercard debit network was provisioned by Mastercard. This is true regardless of the other debit networks for which it is enabled. Thus, if a merchant wishes to process a token provisioned for a debit card that is enabled for Mastercard and Pulse, or one enabled for Mastercard and STAR, and so on, the token itself was provisioned by Mastercard. Mastercard has the power to inhibit merchants' ability to route to any of these competitive networks for every transaction processed on any of these tokenized debit cards.

Mastercard's tokenization policies have to date had a significant impact on our respective members, as they have been forced to route tokenized CNP transactions solely over the

[12] Draft Complaint, para. 36. As will be seen below, the same is true for the tokenization policies that Mastercard plans to implement if the settlement is finalized in its present form.

Mastercard network and thus deprived of the benefits of a competitive market which was the intended result of Regulation II. In this sense, we are very appreciative of the FTC's decision to take action to address Mastercard's actions which the FTC agrees are illegal and violate Regulation II. We are concerned, however, that the remedy negotiated between the FTC and Mastercard will not correct the situation, and Mastercard will continue to deprive merchants of their debit routing choice.

The Proposed Settlement Between the FTC and Mastercard

The proposed settlement tentatively agreed to between the FTC and Mastercard requires Mastercard to provide the competitive networks with the 16-digit PAN in response to a call-out. But it notably does *not* explicitly require Mastercard to inform the competitive networks whether the transaction passed either of the anti-fraud measures built into the industry-wide tokenization specifications: authentication of the cryptogram and domain restriction verification. We understand that Mastercard has since taken the position that it *will* continue to inform the competitive networks whether these anti-fraud measures were passed for CP transactions, but *will not* do so for CNP transactions—continuing to treat these transactions disparately despite the FTC's efforts and notwithstanding the recent pronouncement by the Federal Reserve that issuers *and* networks must each afford CNP transactions the same routing protections as CP transactions.[13]

Mastercard's position plainly inhibits merchants' ability to choose the network they use for CNP transactions and does not comply with Regulation II as explained below. In fact, because the proposed settlement requires Mastercard to comply with all aspects of Regulation II, in our view Mastercard's position violates the proposed settlement. But, if the FTC does not make that clear, Mastercard will continue to violate Regulation II and thwart competition for CNP transactions until such time as the FTC brings another enforcement action – or clarifies that Mastercard must provide the cryptogram and domain restriction information that it provides for CP transactions when it detokenizes CNP transactions.

As discussed above, when a token is detokenized, there are two security checks run—authentication of the cryptogram and verification of the domain restrictions—to ensure that the transaction is legitimate. In the first of these, during a transaction, the token service provider receives a cryptogram that was generated by the customer's device at the time of purchase. It then compares that cryptogram to information regarding the device onto which it originally provisioned the token, ensuring they are the same. Since only the token service provider that originally provisioned the token has information about that device, only it can perform this comparison to verify that the device is authentic. Here, that is Mastercard, since the issuer chose it as its token service provider. And Mastercard, under its existing *and* announced future policies, refuses to do so for CNP transactions when processed over the competitive networks.

[13] Federal Register, Vol. 87, No. 195, p. 61222, n. 24 ("The final rule specifies that card-not-present debit card transactions are a 'particular type of transaction' for purposes of Regulation II's prohibition on network exclusivity as applied to debit card issuers in section 235.7(a)(2). The Board emphasizes that card-not-present debit card transactions are 'electronic debit transactions' for other Regulation II purposes, including Regulation II's prohibition on network exclusivity as applied to networks in section 235.7(a)(3), and prohibition on routing restrictions in section 235.7(b).").

The second security check is the domain restriction verification, during which the token service provider confirms that the transaction complies with the restrictions that it placed on the token at the issuer's request when it was first provisioned (e.g., whether the token is authorized to conduct e-commerce transactions). Again, since only the token service provider is aware of the various restrictions it placed upon the token when it was provisioned, only it can perform this verification. And again, Mastercard has announced its intention not to inform the competitive network whether the transaction passed this anti-fraud check.

As part of the authorization process, whichever network processed the transaction is supposed to inform the issuer, in accordance with industry-standard specifications, whether these two security checks were successfully passed. If it does not or cannot do so, the issuer will *at best* degrade the transaction, assigning it a lower fraud score and increasing the odds that it will be declined. That is, even if the issuer does not reject all of these transactions, issuers will not treat transactions the same regardless of whether these fraud detection tools are applied.[14] If the issuer is informed that a transaction passed the two anti-fraud tests, it by definition means that it is less likely that the transaction is fraudulent. This will then improve the transaction's fraud score and the chances that it will be approved. The converse, of course, is also true. If the issuer is not informed that the transaction passed the fraud checks, or believes that the fraud checks were never applied, it will lower the transaction's fraud score and the odds of it being approved.

By sending through the cryptogram and domain restriction verification to the issuer for its own transactions, but precluding the competing networks from communicating this information to the issuer for transactions processed over their networks,[15] Mastercard is lowering the authorization rates of the competitive networks as compared to its own. The proposed settlement does not clearly address this issue and Mastercard has made clear that it will not do anything to remedy this issue based on the proposed settlement. Since the FTC publicly announced the proposed settlement, it is our understanding that Visa has also taken the position that it will continue to provide cryptogram authentication and confirmation of the domain restrictions *solely* for CP transactions and *not* CNP transactions. This will likewise result in lower authorization rates when the merchant chooses to process a transaction over the competitive networks in those instances where the issuer chose to ask Visa to tokenize the PAN.

Any Token Issued by Mastercard is Subject to the Routing Restrictions of Regulation II

The Federal Reserve Board has recently made clear the routing requirements of Regulation II apply to "information stored inside an e-wallet on a mobile phone or other device."[16] It further noted that if a token falls within the definition of a "debit card," it is subject to these routing requirements.[17] This definition includes "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

[14] If Mastercard were to argue otherwise, the FTC should put it to the test by asking Mastercard, as part of the settlement, to agree *not* to send confirmation of the cryptogram or domain restrictions to issuers with transactions processed over *its own* network.
[15] As noted earlier, only the entity that provisioned the token can perform these anti-fraud tests.
[16] Federal Register, Vol. 87, No. 195, p. 61224.
[17] Federal Register, Vol. 87, No. 195, p. 61224.

regardless of whether the issuer holds the account."[18] Plainly, any token that can process debit transactions over the Mastercard network falls within this definition, and any such token must be enabled for two unaffiliated debit networks for all transactions—*every bit as much for CNP transactions as for CP transactions*.[19]

Mastercard's Own Rules Confirm the Importance of Cryptogram Verification

Mastercard is in no position to argue that the absence of the cryptogram will have no effect on authorization rates. This is clear from its own rules which require that the cryptogram be authenticated whenever a transaction is processed over the Mastercard network:

> The Mastercard Token cryptogram, when present, must be validated during the authorization of all Transactions involving Tokenized Accounts.[20]

Further, any argument that Mastercard should not be required to undertake the obligation to provide authentication of the cryptogram to competitive networks is belied by its own rule requiring *other* token service providers to provide *Mastercard's* Maestro network with verification of the cryptogram authentication on request:

> If Maestro is issued on a debit card other than a Debit Mastercard Card, and the other brand enabled on that debit card offers Tokenization services, the Issuer of the Maestro Account must ensure that the other Token Vault can support and respond appropriately to Token mapping and cryptography validation requests sent by the Corporation to the Token Vault with respect to single message transactions routed to the Interchange System.[21]

Mastercard's Conduct Violates 13 CFR § 235.7(a)(1)

Regulation II provides in part:

> An issuer or payment card network shall not directly or through any agent, processor, or licensed member of a payment card network, by contract, requirement, condition, penalty, or otherwise, restrict the number of payment card networks on which an electronic debit transaction may be processed to less than two unaffiliated networks.[22]

The tokens issued by Mastercard in its role as a token service provider can be processed over the Mastercard network without fail, as Mastercard informs the issuer whether the transaction passed the two industry-standard fraud checks. But, since Mastercard refuses to confirm this fact to the competitive networks when merchants attempt to route over their networks, the competitive networks cannot confirm to the issuer whether the token presented is on the device onto which it was originally provisioned (the cryptogram), or whether it is being used in accordance with the

[18] 12 CFR § 235.2(f)(1).
[19] Federal Register, Vol. 87, No. 195, p. 61224 ("The final rule specifies that card-not-present debit card transactions are a particular type of transaction to which the prohibition on network exclusivity applies.").
[20] Mastercard Rules § 6.1.4(7).
[21] Mastercard Rules § 6.1.4.1.
[22] 12 CFR § 235.7(a)(1).

restrictions placed upon it by the issuer (the domain restrictions). The reason the competitive networks cannot do so is *not* because they independently lack this capability, but because Mastercard—as the entity chosen by the issuer to provision the token—is in sole possession of the information necessary to do so.

If, as a result, the issuer rejects *any* transactions, Mastercard's conduct violates Regulation II since it will be "restrict[ing] the number of payment card networks on which ***an electronic debit transaction*** may be processed to less than two unaffiliated networks."[23] As discussed above, it is a certainty that the lower fraud scoring resulting from the absence of this information will result in an increase in declined transactions over the competitive networks, and thus restrict the number of networks over which those transactions may be processed to fewer than two unaffiliated networks in violation of Regulation II.

Mastercard's Conduct Violates 13 CFR § 235.7(c)

Regulation II provides in part:

> An issuer or payment card network shall not, directly or through any agent, processor, or licensed member of the network, by contract, requirement, condition, penalty, or otherwise, inhibit the ability of any person that accepts or honors debit cards for payments to direct the routing of electronic debit transactions for processing over any payment card network that may process such transactions.[24]

Mastercard's refusal to provide confirmation that the cryptogram and domain restrictions were verified violates this provision of Regulation II in three ways.

First, if it results in *any* transactions routed over the competitive networks being declined, which it invariably will for the reasons stated above, Mastercard will be inhibiting the ability of merchants to direct the routing of transactions for processing over the competitive network for which the card was enabled.

Second, one of the main benefits of token use is the reduction of fraud. And much of that reduction can be attributed to authentication of the cryptogram and domain restrictions. Mastercard's refusal to provide this information means that, when transactions are processed over the competitive networks, the issuer will be required to make an authentication decision without one of the main tools otherwise available to it. Setting aside the endemic risk of fraud that could arise from the removal of this protection, much of the fraud risk for *CNP* transactions falls on the merchant. The increased chances of fraud, and increased chargebacks for which merchants will be responsible, will inhibit their use of the alternative networks. This is not due to any deficiency in the fraud detection capabilities of the alternative networks; the increased fraud arises from Mastercard's refusal to perform its duties as a token service provider in an effort to benefit its own network.

[23] 12 CFR § 235.7(a)(1) (emphasis added).
[24] 12 CFR § 235.7(b).

Third, merchants generally operate on very low margins, and they cannot risk losing sales. One of the primary concerns of e-commerce retailers is what is known as "cart abandonment," which is when a customer loads items into their electronic shopping cart but does not then purchase those items. One circumstance in which cart abandonment often arises is when the customer's efforts to pay for their purchase is declined. When this occurs, they may simply decide not to proceed with their purchase, or instead try to purchase the item at a different e-commerce merchant—only a few clicks away. If processing transactions over the competitive networks results in lower authorization rates due to Mastercard's refusal to verify authentication of the cryptogram and domain restrictions, merchants will be compelled to route transactions over Mastercard in lieu of the competitive networks. Mastercard will again be inhibiting the ability of merchants to direct the routing of transactions for processing over the competitive network for which the card was enabled.

This is not a theoretical or uncertain outcome. In fact, Visa violates Regulation II today by providing the PAN to competitive networks but refusing to provide confirmation of the cryptogram and domain restrictions. The result has been that merchants have been forced to route all tokenized debit transactions on cards with Visa as one of the networks to Visa. The result arising from Visa's practice is nearly identical to the result from Mastercard's existing policy challenged by the FTC. While Mastercard's refusal to even provide the PAN to competitive networks is a clearer bar to competition, Visa's is similarly effective – and Mastercard has made clear that it will simply default to Visa's violative conduct once the proposed settlement is finalized. To the extent the FTC intends to finalize the settlement as-is, then wait to see whether Mastercard's new policy results in merchants obtaining the debit choice to which they are entitled, it need not do so. The years-long experience with Visa already establishes that it will not achieve this objective.

Mastercard's Conduct is a Deceptive Business Practice

Entities across the payments industry *including Mastercard* tout the security benefits of tokenized transactions. Yet these benefits will not be realized on many tokenized transactions if the settlement is approved in its present form and Mastercard is permitted to enact its policies that continue to discriminate against CNP transactions. Most merchants will falsely believe they are able to receive the benefits of Regulation II when they in fact are not—solely as a result of Mastercard's conduct.

Conclusion

The FTC launched this investigation to ensure that Mastercard finally complied with Regulation II and treated tokenized CNP transactions the same way as tokenized CP transactions given that the regulation applies equally to both types of transactions. Unfortunately, Mastercard believes the agreement tentatively reached with Mastercard does not require it to do so. The tokenization policies Mastercard plans to enact if the settlement is finalized in its current form discriminate against CNP transactions, and cynically directly contradict Mastercard's own policies prohibiting other token service providers from engaging in the exact same conduct. The FTC should not permit Mastercard to continue to engage in tokenization practices that treat CNP transactions in a manner inferior to CP transactions, as that not only flies in the face of the FTC's goals in pursuing this investigation, but also the recent pronouncement of the Federal Reserve that the

two types of transactions should be treated equally. We respectfully request that the FTC modify the terms of its proposed settlement to clearly require Mastercard to provide the merchants and acquirers originating a transaction, the network selected by those merchants or acquirers, and other persons authorized[25] by these entities with the PAN (or any substitute account identifier adopted by the issuer),[26] along with confirmation as to whether the cryptogram is authentic, and the transaction complies with the domain restrictions in response to any request relating to an electronic debit transaction as defined in Regulation II.[27]

We are happy to meet individually or jointly at any time to discuss these issues further.

Sincerely,

Merchants Payments Coalition

[25] The order proposed by the FTC, in its current form, requires Mastercard to only provide the PAN to "authorized" entities, defined as those "trained" by Mastercard. Payment network participants should not be subject to this requirement as a condition of exercising their right to route debit transactions under Regulation II, particularly as Mastercard may argue it is entitled to choose whatever "training" it wishes to require.

[26] The purpose of this addition is to ensure that Mastercard and issuers do not agree to use an alternative form of account identification that would circumvent the settlement.

[27] Paragraph II.A of the proposed order extends only to e-commerce, card-not present transactions. The order should apply to *all* electronic debit transactions, as does Regulation II.