August 11, 2021
Ann E. Misback
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551

RE: Fiserv Response to Regulation II; Docket No. R – 1748, Debit Card Interchange Fees and Routing

Ms. Misback:

Fiserv, Inc. (NASDAQ: FISV) appreciates the opportunity to comment on the Notice of Proposed Rulemaking (NPR) issued by the Board of Governors (Board) clarifying Regulation II's debit card routing requirements.

As the Board's NPR notes, the data it has collected from debit card issuers, debit card networks, and other industry stakeholders shows that, as of 2019, two unaffiliated debit networks are not generally available for over 90 percent of card-not-present (CNP) debit transactions that occur in the United States, despite the data also showing that single message networks have developed CNP routing capability. This lack of routing optionality was even more acute in 2020 during the COVID-19 pandemic, when so many Americans turned to online, CNP transactions to purchase basic goods such as food and other staple items.

Fiserv believes that a competitive debit network market benefits card issuers, merchants, and consumers. As a result, we support the Board's efforts in this NPR to clarify that CNP transactions are subject to the same routing options as card present transactions. As the digital transformation continues to accelerate and move an ever-growing percentage of the economy online, a failure to require two unaffiliated networks on CNP transactions — as we believe was intended by the Durbin Amendment within the Dodd-Frank Wall Street Reform & Consumer Protection Act (Dodd Frank) — will result in the shuttering of smaller networks that cannot sustain their economic models on card present volume alone. This would be particularly problematic for debit card issuers, because a lack of competition will drive up prices and minimize the incentive for the surviving networks to invest in more innovative products and services for their issuer partners.

While Fiserv supports the underlying intent of this clarification, we are concerned that a few areas within the NPR may be misconstrued, which could result in a circumvention of Dodd Frank's original intent to create a competitive market for both issuers and merchants, and of the Board's work in this NPR to clarify the law. We therefore appreciate the opportunity to provide our feedback and suggest two additional areas for refinement as you work to finalize this rule.

About Fiserv

Fiserv is a global leader in financial services enabling technology and payment processing, and we interact daily with financial institutions of all asset sizes, businesses, and individual consumers. We are a leading account processor, commonly referred to as a "core" provider, delivering digital solutions to financial institutions in the United States, as well as a provider of many other services including digital

banking solutions, card issuer processing and network services, payments, e-commerce, merchant acquiring and processing, and the Clover® cloud-based point-of-sale solution.

STAR and Accel Historical Perspective and Product Offerings

Fiserv owns the debit networks STAR and Accel, which are two of the traditional PIN debit networks (the "competitive networks"). When STAR and Accel were first formed, in 1984 and 1985 respectively, they could each only process PIN-authenticated debit transactions at a physical point-of-sale terminal.[1] However, as the payments system evolved, so did STAR and Accel.

Before 1990, the number of merchants that accepted debit cards was limited, at least by today's standards. Then, in the early 1990s, acceptance grew rapidly as grocery stores and other types of businesses started for the first time to accept credit and debit cards. Acceptance accelerated further in the early 2000s, as fast-food restaurants also began accepting payment cards. But fast-food restaurants and other rapid-serve businesses required that transactions be processed rapidly. They did not want to slow down their customer flow by requiring either a PIN, as required by the competitive networks, or a signature, as required by the global networks -- Visa and Mastercard. The global and competitive networks solved this dilemma by waiving the requirement for the cardholder to physically sign or enter a PIN on transactions below a preset amount. As ecommerce began to develop, Visa and Mastercard also eliminated the signature requirement for these transactions, as they had previously for other CNP transactions such as mail-order and telephone-order. But while these efforts gave the global networks a jumpstart on the processing of CNP transactions, the threat of competition was looming.

In 2010, the enactment of Dodd Frank led to the release of Regulation II, requiring that each debit card be enabled for two unaffiliated networks. With the expectation that Regulation II would result in their networks being enabled on more debit cards, the competitive networks invested significant resources in developing authentication features that could compete head-to-head with those offered by the global networks. In particular, the competitive networks including STAR and Accel developed features that enabled them to process CNP transactions -- which were previously the exclusive domain of the global networks. Each of the competitive networks realized the increasing importance of this competitive battleground, as CNP transactions continued to grow exponentially. STAR introduced STAR Access, while Accel introduced ANP+.[2] Both solutions are able to support a variety of card present and CNP transactions without a PIN, including incremental payments, aggregated payments, offline environments, multiple shipments, health spending and employee benefit transactions, and rapid throughput transactions such as transit.

The addition of these CNP solutions several years ago means that STAR and Accel have the technical capacity to process every transaction conducted on a STAR or Accel enabled debit card at any merchant location nationwide, regardless of the type of transaction, type of merchant, or where they are located. Additionally, both networks continue to streamline and simplify the enablement process for these

[1] The competitive networks' support of PIN authentication dates back to when they were each originally formed as an ATM network. Banks mandated the security features and required both a physical card and a PIN to access funds in the depositor's accounts. This compared to the signature authentication provided by the global networks. As ATM cards began to serve as debit cards, the competitive networks maintained the additional level of security via PIN entry until market forces and technological developments dictated otherwise, as discussed below.

[2] At the time, STAR was owned by First Data Corporation, which has since been acquired by Fiserv.

solutions, so that they may be easily implemented by issuers. Other competitive networks such as PULSE, Shazam, and others have developed similar CNP features and offer them to issuers today.

In tandem with these CNP solutions, STAR and Accel also developed new, sophisticated fraud detection systems, allowing both networks to catch fraudulent transactions even without PIN authentication. For instance, STAR led the industry in developing a machine-learning fraud score provided to the issuers in real-time as an advanced step in fraud prevention. Analyses conducted by STAR and Accel conclusively show that their CNP transactions are in the same general range for gross fraud loss as that of the global networks.

In developing their CNP capabilities — again, in order to remain competitive in the US payments market as transaction volume shifted from physical stores to eCommerce purchases — STAR and Accel believed that Regulation II's requirement that each debit card be enabled for at least two unaffiliated networks would mean that issuers would have a more robust network marketplace with which to partner for network services, and merchants would truly have a choice between two unaffiliated networks for each transaction.

Unfortunately, that has not been the case and, as the Board acknowledges, "merchants are often not able to choose from at least two unaffiliated networks when routing card-not-present transactions."[3] While virtually all issuers have enabled the global networks' CNP features, the same is not true for the CNP features offered by the competitive networks. And, when an issuer solely enables CNP functionality for one of the global networks, the merchant must route all CNP transactions solely to that one global network. There is nothing the merchant can do to protect its routing choice.

Fiserv's Perspective on Key Components of the NPR

Fiserv interprets the Board's NPR as clarifying issuers' responsibility under Dodd Frank and Regulation II to enable the CNP features offered by at least two unaffiliated networks on each debit card and restricting issuers and networks from taking actions that would inhibit the merchant's ability to route transactions over either network. Again, as transactions increasingly shift to the CNP environment, maintaining a competitive debit network benefits issuers and merchants alike. While issuers receive interchange fees from the merchants when debit cards are used by consumers, issuers pay switch fees to the network that processed the transaction. Competition among debit networks keeps these switch fees competitive. It is ultimately in the best interest of issuers to safeguard a strong, diversified network market. However, as noted earlier, the longer the competitive networks are limited in their ability to engage in CNP transactions, the harder it is for these networks to compete and exist.

The availability of multiple networks likewise supports continuous improvement in quality and features across all networks. If a debit network has high rates of fraud or drives a high level of customer chargebacks or consumer dissatisfaction, merchants will stop directing transactions to that network and instead route them to the alternative network on the card, and issuers will stop enabling that network on the card and instead enable one of the others available. This routing choice and resulting debit network competition ensure that not only will pricing be competitive for both sides of the market, but that networks will strive to provide better fraud prevention solutions, uptime, and overall better service to merchants and issuers.

[3] Federal Register, Vol. 86, No. 91, p. 26190.

Fiserv firmly believes that networks must create a value proposition that works both for issuers to join the network and for merchants to accept the network. However, the only way that a merchant can benefit from such a value proposition offered by a network for various types of debit transactions is if the ***issuer*** enables those options by turning on CP and CNP capabilities of the networks it joins. In other words, federal law requires issuers to enable at least two networks, and the issuer may use various factors such as economics, network capabilities, risk and fraud, etc. in determining which network to enable. But after enabling two (or more) networks, the issuer is prohibited by law from then deciding which transactions can — and which cannot — be routed over the networks that it selected. Under Regulation II, that is up to the merchant.

The problem is not that merchants have not been sufficiently incentivized to route to the competitive networks or that PINless capabilities offered to issuers by the competitive networks are untrustworthy or untested. After all, PINless transactions have been occurring in the quick service restaurant segment for nearly a decade. The problem is that if issuers do not enable a competitive network in the first place (which is the very reason for the Board's NPR), merchants cannot choose to route a CNP transaction over a competitive network because there is no competitive network from which to choose. Networks certainly do have to incentivize merchants to process transactions over their network, since routing choice is (supposed to be) in the merchant's hands. And the competitive networks do so by offering better pricing to merchants. But those incentives are for naught if the issuer hasn't enabled the network to process both CP and CNP transactions, as the merchant simply can't route CNP transactions over the network even if it desires to do so.

Some industry stakeholders have raised concerns with the NPR by suggesting that an issuer would bear liability under the law if the merchant or its payment services provider doesn't support all of the networks enabled on issuers' cards or doesn't support all forms of authentication. We disagree. If a merchant chooses not to support particular types of transactions, or contracts with an entity that chooses not to do so, that is the merchant's choice, which is their right under Regulation II and this NPR. The issuer's obligation is to ensure that, through their own actions, the actions of their agents, and the actions of the networks they choose, the merchant has the ability to interact with at least two unaffiliated networks if the merchant chooses to do so. Given the issuer's control over its own actions and those of its agents, and its ability to select and enable the networks of its choosing, it is fully capable of meeting this obligation. And, if it does not fully enable two unaffiliated debit networks, which is the very subject of the NPR, the issuer has failed to meet its obligation. Concerns about issuers' liability for the actions of merchants is misplaced.

Additionally, some industry stakeholders have expressed concerns about the NPR assigning liability to an issuer if a merchant does not accept a network with a limited geographic area. For a network to qualify as an unaffiliated network for purposes of compliance with Regulation II today, however, it cannot have geographic limitations. That remains the same under the NPR. The issuer's obligation is to enable two unaffiliated networks that are available nationwide, as has been the case since Regulation II became effective.

While we believe the NPR should help resolve some of the routing issues present in the CNP space, we also believe, in the absence of clear direction on certain issues, the Board's NPR could be misconstrued in a manner that deprives merchants from the routing choice afforded them under Regulation II. Fiserv would like to address two issues of particular concern: tokenization and Global AID prioritization.

Tokenization

Tokenization is a process, initiated by a mobile wallet provider or an eCommerce merchant, through which the 16-digit primary account number (PAN) that appears on a physical debit card is transformed by a Token Service Provider (TSP) into a *different* number called a token. Using a token instead of the PAN has several advantages, the most important being security. Specifically, a token cannot be used to produce a fraudulent plastic card since the token must be used in conjunction with a cryptogram and domain channel. Tokenization is an important tool to minimize the costs arising from fraud, and Fiserv strongly supports the use of tokens. As witnessed in recent years, however, tokenization can also be used as a technological weapon to take away merchant debit routing choice.

When a TSP generates a token, it maintains a "look-up table" in which the PAN and its corresponding token are listed. During the processing of a debit transaction, the TSP can use this look-up table to "detokenize" the token, translating it back into a PAN. Detokenization is necessary to process a debit transaction since, in the absence of the PAN, the card issuer is not able to determine the account to which the transaction relates and thus approve or decline the transaction. But since only the TSP that created the token possesses the look-up table, only that particular TSP (or another entity to which it provided the table) can detokenize the PAN. By refusing to detokenize the PAN, the TSP wields full control over the transaction. If it refuses to detokenize the PAN when a transaction is to be processed over a particular network, the TSP also limits competition by preventing other networks on the card from accessing the transaction and thus also limiting merchant routing choice.

When a transaction is conducted using a token, there are also two other data elements that are communicated to the acquirer in relation to the token: the cryptogram and domain channel. The TSP uses these to verify that the token and the transaction are authentic. Since the TSP does this by matching these data elements with those it created at the time the token was generated, this process may only be performed by the specific TSP that originally created the token. This process is critical, as issuers will generally not authorize a tokenized transaction unless they receive confirmation that this matching process was successfully completed.

In short, a TSP has two opportunities to limit routing — by refusing to detokenize a transaction or by limiting access to certain data. Under either scenario, the transaction cannot be processed.

Virtually all of the tokens linked to U.S.-issued debit cards today were provisioned by a global network. This is not due to serendipity or any purported superiority of their tokenization services. Rather, the global networks have required debit card issuers to support their networks' TSP service. Thus, for example, when a mobile phone user seeks to load their debit card into the mobile wallet on their phone, the issuer sends a request to the global network asking the network to provision a token. The token issued by the network is then provisioned on the cardholder's phone instead of a PAN. When that phone is then presented at a merchant location, or the cardholder makes an in-app purchase, the PAN is not visible or otherwise available to the merchant. Rather, the only account number on the phone, and the only account number provided to the merchant, is the token provisioned by the global network. And the only entity that can detokenize the PAN, or authenticate the transaction using the cryptogram and domain channel, is the global network that provisioned the token.

Knowing this, the global networks have used their power, facilitated through these exclusive issuer agreements, to deny merchants' ability to route debit transactions to the competitive networks on the card. One of the networks refuses to detokenize any CNP transactions whatsoever. Additionally, another one of the global networks will provide a PAN for CNP transactions but refuses to confirm whether the

token was verified as authentic through the cryptogram or domain channel. In either circumstance, the issuer will not authorize the transaction. As a result, merchants have no routing control over CNP transactions where the PAN has been tokenized by either of the global networks — which is the case in all mobile wallets. Every CNP transaction conducted with a token generated by the global network TSPs must be sent to the global network that generated the token rather than the competitive network for which the card is enabled.

This conduct has continued notwithstanding the fact that the *existing* Official Board Commentary on Regulation II ("Official Commentary") dated July 20, 2011, provides that the requirement that each debit card be enabled for two unaffiliated networks applies to any token or any application in a mobile phone issued in connection with the card. Here, the global networks, at the issuer's request, have provisioned a token onto a mobile phone, which then constitutes an electronic version of the cardholder's debit card. But the global networks then use the control they have thereby gained when generating the token to preclude merchants from routing over any network other than their own.

It appears that the Board's NPR is attempting to prohibit situations such as that addressed above – stopping TSPs from using their power to inhibit debit routing choice. Specifically, the NPR proposes to amend the Official Commentary, replacing the language above with a requirement that the issuer must enable each debit card for two unaffiliated networks regardless of the means of access. As an example of such means of access, the Board identifies "information stored inside an e-wallet on a mobile phone or other device…"[4]

But, in the same manner in which the Board's earlier language did not preclude the conduct described above, Fiserv is concerned that in the absence of a clear directive on this specific issue, the newly proposed language will similarly be subject to misinterpretation and allow this conduct to continue. For example, a TSP could assert that it is complying with the Board's new language simply by providing the PAN, as one of the global networks now does, notwithstanding the fact that authentication of the cryptogram and domain channel (and confirmation that this authentication has occurred successfully) is also necessary to process the transaction.

Fiserv recognizes that the Board's proposed language is intended to encompass not only current but also future means of access and, as such, it is correctly worded broadly. But the inhibition of routing discussed above is a real-world issue that exists today and is growing exponentially as more and more transactions are tokenized. As such, to ensure that the Board's efforts to preserve routing choice as directed by Regulation II are realized, Fiserv believes that explicit direction is required regarding this issue. Fiserv does not propose amending or replacing the Board's existing proposed language. Rather, it suggests that the Board add language requiring that any issuer, payment card network, or third party provisioning a token, must facilitate detokenization, with all data elements required for authorization decisions, at no cost[5] and without discrimination, for all payment card networks for which the issuer has enabled the card. Alternatively, Fiserv suggests that the Board add additional specificity around what types of network practices would be considered prohibited business practices under Regulation II.

---

[4] Notably, the new language replaces the existing language, *removing* any reference to tokens.

[5] *See* Board of Governors of the Federal Reserve System -- Frequently Asked Questions About Regulation II (Debit Card Interchange Fees and Routing) (https://www.federalreserve.gov/paymentsystems/regii-faqs.htm), § 235.7 Q2. ("Does Payment Card Network A comply with the provisions of section 235.7 if it levies a fee on acquirers for transactions conducted using cards that are enabled for that network but processed over a different payment card network? … No.")

Global AID Prioritization

Each EMV®-enabled debit card issued in the U.S. has two Application Identifiers (AIDs) programmed onto the computer chip embedded in the card. These AIDs tell the application on the chip how transactions should be processed. The global networks own the technology behind each of these AIDs, which are known as the Global AID and the Common AID.

Each of the AIDs on a debit card has the technical ability to process transactions over any of the networks for which the card is enabled. But the global networks refuse to license the Global AID to any network other than their own. As a result, even though a transaction processed over the Global AID could technically be routed to the competitive network for which the card is enabled, the merchant's acquirer is forced to route the transaction to one of the global networks solely due to this licensing limitation. By contrast, the global networks have each licensed the Common AID to the competitive networks, so that acquirers are permitted to route transactions processed using this AID to those networks. This Common AID licensure is how the global networks chose to solve for Regulation II's requirement that the EMV chip facilitate the routing of transactions to at least two unaffiliated networks.

When a chip card is inserted into a merchant terminal at the point-of-sale, the terminal needs to know how to select between the two AIDs that are programmed on the card. One of the methods through which a terminal may be programmed to select the AID is to use the priority given to each of the AIDs by the issuer. Many terminals have been deployed that are programmed to select the AID in this manner, since it is one of the methods authorized by EMVCo, the creator of EMV technology. If a chip card is inserted into one of these terminals, and the Global AID has been prioritized on the card by the issuer, the terminal will automatically select the Global AID. As a result of the global networks' licensing restrictions, the merchant's acquirer will then be forced to route the transaction to a global network only, and the merchant will lose all routing choice.

Additionally, because the global networks have enacted rules mandating that every issuer in the United States must prioritize the Global AID over the Common AID on each of its debit cards, any chance for the competitive networks to win the routing for these transactions is eliminated, regardless of their efforts. Most merchants understandably have no little to no knowledge of EMV routing technology and are unaware of what an AID is, let alone how a terminal selects the AID. As such, few of the merchants that have priority-based terminals are aware of this fact, nor are they aware that they are losing routing control over their transactions.

As with tokenization, the NPR contains language that appears to be directed to preclude the conduct described above. Specifically, the Official Commentary 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.

In Fiserv's view, this language as currently proposed should prohibit issuers from prioritizing the Global AID over the Common AID, because it would constitute an issuer priority that "direct[s] the processing

of an electronic debit transaction" over a single network, depending on the card. The global networks' rules mandating this conduct should similarly fall within the prohibitions of the rule. However, they have in the past taken the position that — by not incurring the expense of replacing or reprogramming their terminals to select the Common AID — merchants have elected to give up their routing choice. As such, there is a concern that the global networks could interpret this new language in a similar manner, claiming that merchants that unknowingly purchased priority-based terminals, and who do not incur the expense to replace or reprogram these terminals, have "chosen" not to designate a routing preference.

To be clear, there is nothing wrong with priority-based terminals. Were the Common AID prioritized on all U.S.-issued debit cards, these terminals would correctly select that AID and routing choice would be preserved for all debit networks. It is only due to the global networks' priority mandate on the issuers that these terminals select an AID that can route to only one of the global networks. Merchants should not be required to expend the time and money necessary to negate the effect of the Global AID prioritization pursuant to the global networks' mandate.

Fiserv's view is that if a prioritization rule must exist, then issuers should only be required to prioritize an AID that can route to any network for which the card is enabled. Moreover, that AID should not discriminate between the networks on the card, for example allowing one network to process biometrically authenticated transactions while the competitive networks on the card are forced to rely solely on PIN authentication -- or no authentication at all. Accordingly, Fiserv suggests that, together with the Board's proposed new language prohibiting network rules or issuer priorities that direct the processing of an electronic debit transaction on a specified payment card network or its affiliated networks,[6] the Board add as an example of this prohibited conduct the prioritization of an AID that cannot route to all networks for which the card is enabled or can only do so in a discriminatory manner.[7]

Since re-prioritizing the AIDs on a debit card requires card reissuance, we anticipate that complaints may be received by the Board regarding the expense of this process. This expense may be ameliorated, however, by setting a future date for full compliance, while requiring that all cards issued in the interim be compliant with the new requirements. Alternatively, there is a method through which this change can be effectuated almost immediately, at little cost. As indicated above, the Global AID is already enabled and prioritized on every U.S.-issued debit card. This AID has the technical capability of processing transactions over any network and doing so on equal footing. The only reason it is not used in this manner is as a result of the global networks' refusal to license the Global AID to the competitive networks. Were they to provide such a license, granting the competitive networks' access to the Global AID on equal footing to their own networks, all existing cards would simply become compliant.

Conclusion

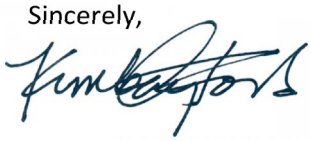
[6] Proposed amendment to Official Commentary, Federal Register, Vol. 86, No. 91, p. 26195.

[7] In addition to the other issues described above, the license granted by the global networks to the competitive networks for the Common AID is limited, restricting the types of transactions that may be routed to these networks. Specifically, both global networks only allow the competitive networks to process transactions that have been authenticated by PIN, or those that have no authentication whatsoever. Again, this is not a technical issue, but arises solely from the global networks' refusal to fully license even the Common AID to the competitive networks. The global networks allow their own transactions to be processed not only over the Global AID, but also the Common AID, without these limitations. Just as Dodd Frank required the addition of an AID to which the competitive networks had access, it should be interpreted to require that this access be provided in a nondiscriminatory manner.

As indicated earlier, Fiserv is supportive of the Board's efforts to ensure that the requirements of Regulation II extend to all merchants and all types of transactions. The comments and suggestions included within are intended to protect competition and access to networks for issuers and merchants alike. In that spirit, we respectfully request that the Board consider the points of clarification discussed above to avoid the necessity of addressing these potential loopholes to the regulation in future rulemakings.

Fiserv welcomes continued engagement with the Board on these issues.

Sincerely,



Kimberly Ford
Senior Vice President, Government Relations
Kim.ford@fiserv.com
(202) 478-1112