FOOD MARKETING INSTITUTE
Feeding Families and Enriching Lives

September 30, 2011

Jennifer J. Johnson, Secretary
Board of Governors of the Federal Reserve System,
20th Street and Constitution Avenue, NW
Washington, DC 20551

Submitted Electronically

Docket No. R–1404; RIN No. 7100 AD 63

Re: Debit Card Interchange Fees and Routing

The Food Marketing Institute (FMI) appreciates the opportunity to respond to the notice and request for comment from the Federal Reserve Board of Governors on debit card interchange transaction fees and routing.

FMI is the national trade association that conducts programs in public affairs, food safety, research, education and industry relations on behalf of its 1,500 member companies – food retailers and wholesalers – in the United States and around the world. FMI's members in the United States operate approximately 26,000 retail food stores and 14,000 pharmacies. Their combined annual sales volume of $680 billion represents three-quarters of all retail food store sales in the United States. FMI's retail membership is composed of large multi-store chains, regional firms, and independent supermarkets. Our international membership includes 200 companies from more than 50 countries. FMI's associate members include the supplier partners of its retail and wholesale members.

In our comments, we will discuss the amount and structure of the Federal Reserve's proposed fraud prevention adjustment and why the proposed levels and structure are inconsistent with the intent of statutory language based on merchant fraud prevention expenditures, merchant fraud loss, merchant liability, and lack of payment guarantee for a merchant in the signature debit card environment. We will also highlight the difference between signature and PIN debit and the impact on the supermarket industry, the importance of stronger fraud prevention standards in the United States with the adoption of mobile payments, the need for strict enforcement of the fraud prevention standards outlined by the Federal Reserve by an independent federal agency instead of reliance solely on network oversight, and the proposed effective date of the interim final rule.

2345 Crystal Drive, Suite 800 • Arlington, VA 22202-4801 • T 202.452.8444 • F 202.429.4519 • fmi@fmi.org • www.fmi.org

Proposed Value and Structure of Fraud Prevention Adjustment

There are many participants in the electronic payments chain: networks, issuers, acquirers, merchants, and consumers. In order to protect electronic payments for all participants in the chain, but in particular consumers, it is critical that the proper incentives exist for each party to invest in the most secure payments technology. FMI, along with Consumer Reports, [1]believes the United States is lagging behind the rest of the world in payments innovation – attributable to the gross inefficiencies fostered by the United States' current interchange fee structures.[2]

The statutory language in Section 920 of the Dodd-Frank Wall Street Reform and Consumer Protection Act is very clear that fraud prevention costs undertaken by all parties[3] in the payments chain should be considered when promulgating a fraud prevention adjustment standard. Based on the Federal Reserve's silence regarding the costs incurred by other market participants, it is clear the Board considered predominately issuer costs in its interim final rule.

We were encouraged by the Federal Reserve's proposed rule that recognized a major technology shift might be necessary to prevent fraud in the United States, but were extremely disappointed the Federal Reserve's final rule rewards market inefficiencies through interchange fee revenue for parties the rule was meant to rein in – financial institutions with more than $10 billion in assets. As expected, all major debit networks committed to support a two-tier debit interchange fee structure for exempt and non-exempt financial institutions, and some networks even raised interchange fees for all issuers one more time in August 2011.

Fraud Prevention Adjustment Fee Structure:

The statute is clear that fraud losses are not to be covered by interchange.[4] Interchange fee revenue that offsets fraud losses for issuers removes the incentive for them to innovate and employ the most secure payment technologies. As such, fraud losses should not be directly incorporated into the interchange fee standard nor assessed as an ad valorem fee. The Federal Reserve should not adopt a rule that supports today's flawed system.

The proposed 5 basis point ad valorem fee adjustment is not appropriate because: 1) it was never vetted in a proposed rule; 2) it incorporates fraud losses, which are not among the "incremental cost incurred by an issuer for the role of the issuer in the authorization, clearance, and settlement of a particular debit transaction"[5] the statute allows the Fed to consider as part of the interchange fee standard; and 3) the fee structure does not take into account the fact that merchants have shared liability for fraud losses, including higher dollar loss risks with higher transaction values if a chargeback is initiated and upheld by the networks and issuers.

---

[1] http://www.consumerreports.org/cro/magazine-archive/2011/june/money/credit-card-fraud/overview/index.htm

[2] http://www.mastercard.com/us/merchant/pdf/TB_CB_Manual.pdf; http://usa.visa.com/download/merchants/visa-international-operating-regulations-main.pdf (Chapter 9, Dispute Resolution)

[3] §920(5)(B)(IV) and (V)

[4] §920(4)(B) limiting the costs to be considered to the "incremental cost incurred by an issuer for the role of the issuer in the authorization, clearance, or settlement of a particular electronic debit transaction."

[5] §920(4)(B)

This rule structure perpetuates a situation wherein a network may require a merchant simultaneously pay a fraud premium on every transaction, and then bear the lion's share of the losses for fraudulent transactions that were initially authorized by the network and issuer. Merchants are not guaranteed payment for debit transactions, so even though they will pay a fraud premium on debit transactions, the issuer and the networks ultimately decide who bears fraud losses through onerous chargeback rules.

The structure of the proposed rule is concerning to the supermarket industry because the 5 basis point ad valorem fee is assessed on both signature and PIN debit, the latter of which is much more secure. Given the industry is one of the highest adopters of PIN debit in the United States, supermarkets are going to be paying for an inordinate amount of fraud losses in the system. Additionally, the 5 basis points fee is inclusive of cashback, which we believe is highly inappropriate and is a policy that could end up limiting a program that has been historically beneficial to both the merchant and customer.

Fraud Prevention Adjustment Value:

FMI does not support the proposed value of the fraud adjustment in the Federal Reserve's interim final rule because increasing the amount issuers are able to collect in interchange will perversely reward issuers for maintaining antiquated systems, rather than providing them with adequate incentives to invest in more secure technologies. Failure to incentivize investment in more secure technologies in the Final Rule will negatively impact both merchants and consumers who have significant liability on debit card payments.

The Final Rule also does not take into account the fraud prevention costs expended by other parties in the payments chain. According to a 2009 Lexis Nexis study that was presented at the November 2009 Kansas City Federal Reserve Bank's Retail Payments Conference, merchants bear nine times the amount of fraud losses borne by issuers or networks.

The fraud prevention adjustment value and structure, combined with the significant disparity between the Federal Reserve's initial proposed interchange fee standard value and the fee standard contained in the Final Rule could cause many merchants in the supermarket industry to incur higher interchange rates as the vast majority of networks have already announced rates that bring all regulated supermarket interchange transaction fees up to the fee cap. We believe the intent of the statute was to reduce costs for consumers, and it is unlikely that higher interchange fees for merchants will bring that to fruition.

Lastly, we reject the concept that transaction monitoring should be covered by merchants via interchange fee revenue since the monitoring encompasses account activity unrelated to merchants—payments and withdrawals of all kinds from a demand deposit account, such as check payments, ACH payments, and ATM withdrawals, and is not limited to just debit card point-of-sale payments. That being said, we were pleased to see that the Federal Reserve did not include transaction monitoring in both the 5bps ad valorem portion of their interchange fee cap and the 1 cent fraud adjustment, and we urge the Fed not to do so when the rule becomes final.

Merchant Fraud Prevention Expenditures, Merchant Liability, and Fraud Loss

In both our comments[6] on the proposed rule and in a November 2010 submission to the Federal Reserve, FMI noted that supermarkets invest significant time and resources in fraud prevention to protect our brand and our customers. The acquiring community, as well, has been seeking innovative solutions, such as end-to-end encryption and tokenization that are meant to help prevent fraud and data theft. While we do not believe these technologies are prescriptive, we do assert that certain parts of the payments chain are more proactively innovating to secure the electronic payments infrastructure than others.

Issuers and networks have historically lacked any real incentive to develop similar innovations, and the Federal Reserve's current proposed interim final rule leaves interchange fee revenues at a level that will not incentivize networks or card issuers to correct their inefficiencies. The current U.S. payments system is inundated with misplaced incentives. Certain stakeholders—banks and networks—profit by steering customers to the least secure transactions, signature debit. Because these transactions are the most profitable for them, and because the issuers and networks dictate their deficient security standards with very limited merchant liability protections, the United States lags behind the rest of the world in the security of its card products—both the viability of the card and card-user authentication—and experiences shortfalls in protecting data in transit.

The Payment Card Industry (PCI) Data Security Standards (DSS) and the PCI Council, which consists of the five major payment card networks, drive many of the payment card security standards in the United States. Despite the fact that merchants spend millions of dollars to comply and maintain compliance with the standards, the PCI council is receptive to very little input from the merchant community. In order to accept any payment card, merchants must conform to the PCI DSS, even though its effectiveness is unproven. What is worse, in the event of a breach, a breach itself nullifies PCI compliance meaning the merchant remains liable despite the fact they were deemed compliant, according to the PCI DSS.

Additionally, these standards, which have existed since 2005, have done little to advance the United States toward a secure payments environment. According to a June 2011 Consumer Reports[7] article, the "United States and some non-industrialized countries in Africa are among the only nations still relying on magstripe payment cards, which came into wide use in the 1970's." The article questions why the United States is so far behind the rest of the industrialized world in migrating to new, more secure payment products and draws the conclusion that "it seems to come down to money. The losses for banks do not yet exceed the costs of a switch-over." Unfortunately, the Federal Reserve's fraud adjustment disincentivizes such a "switch-over" to the detriment of merchants and consumers.

Given the profit-incentives of issuers in today's system, it is not surprising that the United States has been one of the slowest adopters of new payments technology. While Visa recently announced that they are shifting their U.S. cards to EMV (Chip), and dictating liability shift to all non-EMV compliant merchants by 2015 [fuel merchants by 2017], we note that some merchants have been advocating this change for years. Yet, we are concerned with the timeline of the Visa mandate because of the undue burden it could place on small businesses that may not have the access to capital to invest in new Chip-

[6] http://www.fmi.org/newsletters/uploads/CommentsFiled/FMI_75FR81722_021011.pdf
[7] http://www.consumerreports.org/cro/magazine-archive/2011/june/money/credit-card-fraud/overview/index.htm

enabled card readers by the deadline, and we would encourage the networks to consider subsidizing the implementation of EMV in the United States to ensure all parties in the U.S. payments chain are sharing in the cost of making consumer debit card payments more secure for all our citizens. We would also note that the proposed transition time in the United States is much shorter than the transition periods in both Canada and Europe.

Chip and PIN cards, which are prevalent in Europe, Australia, Asia, Africa, South America, Mexico and Canada, require a two-step authentication: 1) the Chip validates that the card in use is not counterfeit; and 2) the PIN validates the card user. According to the same Consumer Reports article a representative from the New York Police Department said they had "recommended to several of the large financial institutions that the biggest deterrent to skimming [illegal copying of magstripe data] would be using the kind of cards that are issued in Europe and Canada with a chip that makes them pretty much impossible to skim, but so far they seem unwilling to do that."[8] Also worth noting with respect to the Visa transition to Chip is that a PIN is currently necessary to authenticate the debit cardholder in most current retail environments today, so the supermarket industry sees little value in the shift to EMV that does not also require the authentication of the card user with a PIN.

While adoption of Chip and PIN and other more secure technologies has been slower in the United States than in any other industrialized country in the world, the current PIN debit product is still significantly more secure than signature debit. However, there is still evidence of issuers, such as JP Morgan Chase, steering customers to use signature[9], thus supporting our earlier point about a lack of innovation on the network and issuer side of the payments chain. It is important to note this is not a new phenomenon. As early as 2002, consumer advocates said consumers were better off punching in a PIN for check-card transactions. Bill Apple of Consumer Reports told Bankrate.com: "We generally don't like these cards with a signature. They're not as secure. Also, if people sign, the bank collects much higher fees and ultimately it will raise the cost of goods and services for everyone. The merchants will be paying higher transaction fees, and that's coming out of overhead somewhere. Eventually, they may have to jack up prices."

Another shortfall of signature debit is network rules that prohibit merchants from declining a sale even if the customer's identification does not match the name on their card[10]. If the merchant refuses the network brand or card based on an ID check, they risk losing their ability to accept Visa or MasterCard.[11] Given the existence of this rule, as well as issuer and network control over card products, we reject the Federal Reserve's assumption that "network rules that are vague with respect to merchant requirements for authenticating a signature may lead to fraud losses being borne by the issuer when the merchant was in a position to compare the cardholder's signature with the signature on the back of a card and prevent the fraud."

Lastly, one of the largest security threats occurs when data is in transit. However, according to a September 2009 issue of the *Nilson Report* (Issue #934), networks cannot accept encrypted data, which

---

[8] Ibid.
[9] Counterintuitive Pitch for Higher-Fee Debit Category. *American Banker*. April 20, 2010 http://www.americanbanker.com/issues/175_75/debit-1017958-1.html
[10] See Visa Operating Rule 5.1.D.1.a – Validation of Cardholder Identity stating that the "signature may be different from the name embossed or printed on the Card.
[11] See Visa Operating Rules, Page 449 "Supplemental Identification – U.S. Region" prohibiting merchants from requiring any "supplementary Cardholder information as a condition for honoring a Visa Card…"

requires data in transit to be decrypted, exposing it to risk. Innovation by networks and issuers in this space could likely reduce fraud and should be included as part of the fraud prevention adjustment requirements. As noted earlier, acquirers have been working on market solutions to protect data in transit. In the current marketplace, they have the incentives to do so to better protect themselves and their merchant clients from a breach and breach liability, but the current marketplace has fostered no such noticeable innovation to date on the part of the networks and issuers.

The Board's decision to allow issuers to recover fraud losses through interchange transaction fees is not reasonable given the lack of innovation on the network and issuer side of the payments chain, along with the fact that the statutory language does not permit it. A card product originates with the issuer under the rules established by the network and is processed via network rails, yet, there has not been any significant fraud deterring innovation in this part of the payments chain for decades. The banks and networks control two of the most critical elements in payment card security -- card user authentication and safe transfer of data - so any claims that the merchant is in the best position to address fraud are completely unfounded.

Merchants are largely unable to influence the technology on a debit card or the way card information is shared. Furthermore, because merchants do not have a guarantee of payment when a debit card is used, they face increased risk liability as the transaction amount goes up just as issuers do. For this reason, an ad valorem fee is highly inappropriate for addressing fraud losses as long as network-mandated chargeback rules prevail in the marketplace. Unfortunately, because these rules allow issuers to continue to recover losses on fraud prone signature transactions and because the Federal Reserve's proposed interim final rule affords issuers the ability to recover the costs of "initiating, receiving, and processing chargebacks, adjustments, and similar transactions" and the costs of "receiving and processing presentments of electronic debit transactions,"[12] as part of the interchange fee standard calculation, it is unlikely issuers or networks will change them any time soon. FMI is extremely disappointed that the interim final rule not only covers fraud losses, but also does not deter issuers from initiating chargebacks in any way, especially when there are certain types of chargeback codes (i.e., counterfeit) that merchants have no ability to challenge.

Product Authentication & PIN in the Supermarket Industry

Traditional brick-and-mortar supermarkets are in a unique position compared to other merchants impacted by the debit card interchange fees and routing rules, and in particular the fraud prevention adjustment, because the supermarket industry is one of the largest adopters of PIN transactions. According to the 2010 Pulse Debit Issuer study, 39% of PIN transactions in the United States are at supermarkets, so fraud for our industry is likely much lower than in some other retail segments. However, the Federal Reserve's final rules on the debit interchange fee standard and routing may increase costs for some merchants in our industry as some PIN rates from early 2011 are lower than the 21 cent cap even without the fraud adjustment standard. With the 5 basis point ad valorem fee and the one cent fraud adjustment fee on all types of transactions, segments of our industry will likely end up paying significantly higher debit card interchange fees, contrary to the intent of the statute. By disregarding the investments made by the supermarket industry and the current rates that supermarkets

[12] See Federal Reserve Final Rule Commentary, page 167

pay, the Federal Reserve has potentially increased costs for supermarkets — and thus consumers — and reduced the incentives issuing banks have to combat fraud in the system.

Given the lower fraud rates on PIN debit compared to signature, FMI expects the inclusion of PIN capability will be a prerequisite for an issuer to receive any fraud expense adjustment for any type of access to a debit account, including via mobile payments, at least until a more secure account user authentication method is created and substantiated. Absent such a requirement, banks will continue to abuse their power over the payments system, as they have done in Minnesota, where debit cards are not currently PIN-enabled.

FMI also strongly encourages any EMV (Chip) technology standard to empower merchants to require entry of a PIN. If merchants are to be faced with a liability shift within the next three years, the technology shift should be a proven deterrent against fraud, which EMV signature is not. Supermarkets account for much of the current acceptance of offline Chip cards in the United States via our participation in the Women, Infants, and Children (WIC) Electronic Benefits Transfer program in certain states such as Texas. Because of this widespread acceptance, it is also our hope that network branded Chip technology in the United States will be compatible with the point-of-sale equipment already in place in some merchant locations.

Certification & Enforcement

FMI strongly urges the Board to adopt a certification procedure to ensure both networks and issuers are complying with the Board's fraud prevention standards in order to receive or charge the fraud prevention adjustment beginning October 1, 2011. Network certification of the fraud prevention adjustment amounts to an unacceptable conflict of interest, as networks compete for business from the very issuers of which they would be certifying.

It is important that the Federal Reserve or another agency take responsibility for certifying the security of a particular technology or practice and whether or not adoption of that technology meets the fraud prevention adjustment standards. For example, we have noted an EMV signature transaction (as opposed to an EMV PIN transaction) may not deter fraud as much as current PIN magstripe transactions. Additionally, as FMI noted in our comments on the proposed debit card interchange transaction fee and routing rules, networks have in the past mandated unproven technologies such as Triple Data Encryption Standards (TDES) that are costly to implement and may not serve as an added theft deterrent. In addition to oversight, the Federal Reserve should promote transparency by requiring that all fraud prevention adjustment data be submitted to the Federal Reserve and open to public inspection.

Finally, we believe the adoption of mobile payments affords the United States an opportunity to become a world leader in fraud prevention standards. To date, uptake in the mobile payments arena has been slow, primarily due to the duopolistic nature of the payment card market in the United States. The new debit transaction fee and routing rules will hopefully enhance competition in the mobile payments space, and possibly speed up adoption. In order to avoid costly add-ons in the future, though, it is critical that effective fraud prevention and security standards be created in the early years of mobile in the United States. For the benefit of all U.S. merchants and consumers, FMI strongly encourages the Federal

Reserve to adopt a higher fraud prevention standard for mobile payments than it has with existing magstripe debit card products.

Effective Date

FMI believes October 1, 2011, is a realistic effective date for the final rule on the reasonable and proportional standard. , Networks already took the opportunity to raise rates during the implementation delay period. Since it is only large financial institutions with assets greater than $10 billion who are covered by the rule, it is critical for all those institutions to be certified by the Federal Reserve as having met their fraud prevention standard in order to receive the adjustment for fraud prevention as of October 1.

Thank you in advance for the opportunity to provide feedback on the Federal Reserve Board interim final rule on the fraud adjustment provisions of the debit card interchange transaction fee and routing rules.

Sincerely,

Jennifer Hatcher
Senior Vice President, Government Relations
Food Marketing Institute