Joshua R. Floum
General Counsel

By Electronic Delivery

September 30, 2011

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

Re: Docket No. R-1404, RIN No. 7100—AD 63, Debit Card Interchange Fees and Routing

Ladies and Gentlemen:

This letter is submitted on behalf of Visa Inc. ("Visa") in response to the interim final rule ("Rule"), published by the Board of Governors of the Federal Reserve System ("Board") in the Federal Register on July 20, 2011. The Board has requested public comment on the Rule, which it adopted in accordance with Section 920(a)(5) of the Electronic Fund Transfer Act ("EFTA") relating to adjustments to debit interchange transaction fees for fraud prevention costs. Visa appreciates the opportunity to comment on this important matter.

Visa understands that the fraud-prevention adjustment included in the Rule is discretionary under Section 920(a)(5) and strongly supports the Board's decision to adopt the fraud-prevention adjustment. Visa believes that the Board should permanently adopt an appropriate fraud-prevention adjustment. Fraud is a continuing concern in all types of payment transactions. Efficient markets, both wholesale and retail, require efficient, reliable and secure methods of making payments in order to complete transactions. Simply put, merchants will not want to accept a form of payment unless they are confident that payment will be made as agreed, and consumers will not use a form of payment that merchants will not accept or that puts them at risk of fraud.

As a central bank with payment system responsibilities, it is appropriate for the Board to recognize the importance of preventing fraud in electronic debit transactions and to use its authority under Section 920(a)(5) to provide for a fraud-prevention adjustment to regulated interchange transaction fees. The fraud-prevention adjustment will serve not only to compensate issuers for costs incurred in undertaking fraud prevention programs, but also to further establish fraud prevention as a business and regulatory priority in electronic debit transactions. Making fraud prevention a priority in these transactions should contribute to both consumer and merchant confidence in electronic debit transactions, as well as other retail electronic payments. In order to promote this confidence most effectively, it is important for the Board's fraud-prevention adjustment standards to recognize the dynamic nature of fraud and to allow, and encourage, issuers to adopt holistic fraud prevention programs that recognize and respond to the evolving character of the threat of fraud and that address the threat proactively, without artificial constraints that skew fraud prevention programs toward perceived, but exaggerated, threats. For

Visa Inc.
P.O. Box 194607
San Francisco, CA 94119

jfloum@visa.com
t 415 932 2244
f 650 554 3711

these reasons, and as set forth in greater detail below, Visa strongly supports not only the implementation of a fraud-prevention adjustment, but also the implementation of such an adjustment along the general lines outlined in the Rule. Nevertheless, Visa believes that the wording of the Rule can be improved to reinforce the flexible, holistic approach that the Rule already reflects.

Importance of the Fraud-Prevention Adjustment

Section 920(a)(5) contemplates not only a fraud-prevention adjustment to interchange transaction fees, but also the establishment of standards that must be met for an issuer to qualify to receive the adjustment. As such, Section 920(a)(5) conditions the fraud-prevention adjustment on federal standards for fraud prevention activities at debit card issuers that wish to receive such adjustment. Although the adjustment may not be applicable to institutions with combined assets of less than $10 billion or to debit cards under certain prepaid and government programs, and although the adjustment standards do not apply to credit cards, Visa believes that the standards established by the Board under Section 920(a)(5) are likely to set expectations for fraud prevention by issuers in the payment card industry more broadly. Approached properly, such standards have the potential to encourage robust fraud prevention at payment card issuers and to lay the foundation for effective, evolving fraud prevention programs that respond to changes in the patterns, practices and technologies of fraud as the methods of authorizing payment card transactions develop and evolve.

The importance of effective fraud prevention in retail transactions cannot be over emphasized. Merchants will be reluctant to accept forms of payment where they lack confidence that the payment will be completed as contemplated and that the payment is not fraudulent. At the same time, consumers will not want to use a form of payment that exposes them to liability for, or loss from, fraudulent transactions. Nor will either merchants or consumers want financial institutions to absorb the cost of fraudulent transactions in the long run. A merchant or consumer may prefer that a financial institution absorb the cost of an individual fraudulent transaction, but in the longer run, neither merchants nor consumers will want to pay higher costs for payment services generally. Put simply, it is in everyone's interest to prevent fraud in payment transactions.

Visa has long recognized the importance of preventing fraud in electronic payment transactions. Visa is a leader in information security standards and a provider of important anti-fraud tools to other businesses. Ensuring that Visa payments are convenient, reliable and secure is Visa's highest priority. As a payment card network, Visa believes that it is critical to maintain and strengthen cardholder trust in every Visa transaction. As a result, Visa protects each link within our control and works with others in the payment chain to ensure there is no single point of failure.

Visa has invested heavily in advanced fraud-fighting technologies, and we continue to develop and deploy new and innovative programs that fight fraud and protect cardholders. For example, Visa deploys cutting-edge technologies to monitor payment card transactions on a global basis—24/7/365—in order to spot fraud when it occurs and stop it. Our sophisticated neural networks flag unusual spending patterns that enable financial institutions to block

authorizations for payment card transactions where fraud is suspected. Visa has also partnered with issuers as they layer their own security functions on top of Visa's. This partnership approach has proven to be the most effective way to manage and limit fraud and to expand the usage and acceptance of payment cards by both cardholders and merchants. These efforts have kept fraud rates at historic lows, enabling cardholders to use Visa with confidence. With technological innovations and advances in risk management, fraud rates have declined by more than two-thirds over the past two decades.

In addition, Visa is a founding member of the Payment Card Industry ("PCI") Security Standards Council, which develops the information security standards for the handling of payment card data—the PCI Data Security Standard ("PCI DSS"). PCI DSS was developed to encourage and enhance cardholder data security and the broad adoption of consistent data security measures for cardholder data globally. PCI DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers and service providers, as well as other entities that store, process or transmit cardholder data.

Visa believes that an effective security strategy relies on multiple layers of protection. These layers range from anti-counterfeit measures to neural networks that analyze each transaction in real time. More specifically, Visa takes a total-systems approach to fraud prevention. For example, Visa's own fraud prevention efforts focus on: (1) securing the payment environment to protect card data and render it useless in the hands of unauthorized parties, including potential criminals; (2) managing fraud by protecting cardholders with Zero Liability; (3) maintaining trust through merchant and cardholder education and industry leadership; and (4) creating an environment of partnership by promoting industry engagement and accountability.

The Fraud-Prevention Adjustment

While Visa recognizes that for timing reasons the amount of the fraud-prevention adjustment is fixed for practical purposes for some time after the implementation date of the interchange transaction fee cap of October 1, 2011, Visa believes that the Board should consider changes to the fraud-prevention adjustment going forward. First, Visa believes that most fraud prevention programs are targeted at larger dollar transactions because that is where the risks of loss are most significant. Under the current fraud-prevention adjustment, the 1 cent adjustment would apply to both a $0.75 transaction and to a $1,000.00 transaction. Clearly the fraud risks and level of associated fraud prevention resources applied to these transactions are different and the effects of increasing the interchange rate on these transactions by 1 cent are different. Adding 1 cent to the interchange transaction fee for small dollar transactions allocates fraud prevention costs to these transactions disproportionately and is likely to have the effect of deterring the use of debit cards for smaller dollar transactions. Accordingly, in the future, it may make more sense to set the fraud-prevention adjustment as an *ad valorem* expressed in basis points similar to the fraud loss component of the interchange transaction fee cap, rather than as a fixed amount.

Visa also notes that the fraud-prevention adjustment is calculated to cover the median fraud prevention cost, excluding transaction monitoring costs, while the interchange transaction

fee cap was calculated to cover the 80th percentile issuer's average per-transaction cost. This difference is not explained. Visa believes that for the reasons stated by the Board with respect to the interchange transaction fee cap, in the future the fraud-prevention adjustment should be computed on this same 80th percentile basis. In addition, the Board appears to have disregarded data security costs of 0.4 cents per transaction at the 80th percentile. The 80th percentile number for fraud prevention plus data security less transaction monitoring costs would yield a fraud-prevention adjustment of 2.3 cents. Further, Visa notes that Section 909 of the EFTA recognizes that customer notification to issuers of actual or potential unauthorized transactions is a key fraud prevention task. Indeed, the Board recognized the importance of handling such customer service calls in the Commentary.[1] Accordingly, Visa believes that the Board should include an appropriate portion of the six-cent customer inquiry cost (at the 80th percentile) in the fraud-prevention adjustment to reflect the costs of receiving reports for potential or actual unauthorized transactions.

The Non-Prescriptive Approach to Standards

The Rule requires an issuer to implement policies and procedures reasonably designed to address four separate aspects of fraud and cardholder data security. This approach implements the non-prescriptive approach on which the Board sought comment in December 2010, as opposed to the technology-specific approach regarding which the Board also sought comments at that time. Visa believes that the general non-prescriptive approach as embodied in the Rule is far preferable to the technology-specific approach. Presumably, under the technology-specific approach, the Board would identify technologies and then advise issuers that investment in these technologies could be recovered through interchange transaction fees. As Visa stated in its response to the December request for comment, the technology-specific approach would have a number of significant drawbacks.

First, the technology-specific approach would incorrectly assume that all fraud prevention is based on technology. Procedures, training and awareness also play significant roles in fraud prevention. Most data breaches and resulting fraud are caused by a failure of participants in the payment system to deploy known, existing technologies or industry-standard best business practices (*e.g.*, user access controls, password management, system access monitoring and employee training on all of the above). Focusing on technology alone naively assumes there is a "magic bullet" that, by itself, would result in materially more efficient fraud control.

In addition, the technology-specific approach presumes that the Board is in a better position to identify technologies for investment than the institutions involved in the transactions. Given the inherent complexity of electronic debit payments, including the participation of thousands of U.S. issuers, processing entities, millions of merchants and point-of-sale terminals, numerous vendors for terminals, cards and mobile phones, millions of cardholders and interoperability implications that may arise for international cards and transactions, the Board is not likely to be in a position to assess the commercial feasibility of specific technologies. A potential new technology can only be assessed with hindsight, with trial and error, and long after

[1] 76 Fed. Reg. 43,478, 43,487 (July 20, 2011).

networks and issuers have invested substantial resources and the technology has been tested, broadly implemented and become the prevalent mode of transacting. Creating an incentive structure for issuers and networks to place substantial investment on specific technologies that may be untested, or have uncertain prospects of adoption or success, would likely lead to a number of wrong turns and wasted effort. The initial development of the PCI DSS standards for securing cardholder data evidenced these difficulties. Years spent attempting to determine specific technology solutions led to the conclusion that this approach was unworkable and that the flexibility to combine technology and process solutions would, and did, lead to far more effective security.

The potential to be able to recover costs for only Board-approved technologies would create strong incentives to invest primarily in such technologies, which could result in an inefficient allocation of resources because it would likely discourage investment in other technologies, processes or centralized network solutions that are more effective and less costly. Moreover, the mere identification of technologies that would permit a fraud-prevention adjustment and the resulting industry shift toward their use would alert creative, well-funded and sophisticated wrongdoers to the specific technologies that they must combat. The technology-specific approach also would provide issuers with far less flexibility in order to adapt to changing technologies and fraud patterns, and the Board would need to continually monitor and update the standards as appropriate. A technology-specific approach also likely would require issuer-specific interchange fees for those issuers that adopted the Board-identified technology.

Providing fraud compensation only for specific common, industry-wide technologies would also lead to less issuer and network competition. Effective fraud prevention is one of the factors on which issuers, networks and acquirers may compete. While some solutions require standardization to be widely adopted (*e.g.*, placement of magnetic stripe data), others do not, such as more effective fraud detection tools. For example, Visa has developed and is deploying novel solutions, such as alerts sent to cardholders by text message or e-mail whenever their cards are used and tools that enable cardholders to control use of their cards by placing selective acceptance blocks on their cards (*e.g.*, do not allow transactions at electronic stores or overseas). As wrongdoers target consumers with phishing attacks and identity theft, it will be more critical going forward to engage consumers more directly in controlling fraud. Where a fraud-prevention adjustment is provided only for industry-wide solutions, issuers and networks are likely to focus their investment efforts instead on standardized, undifferentiated solutions. The lack of competitive advantage in homogenous solutions that would be available to everyone tends to mute the incentive for networks and issuers to invest in such solutions, even if they might benefit from the overall growth of electronic payments. For these reasons, Visa strongly believes that the non-prescriptive approach adopted by the Rule is the only viable approach to fraud prevention standards.

Lastly, proscribing a specific common industry-wide technology creates a single point of failure. If wrongdoers can penetrate or compromise this solution, the entire system would be put at risk. The complexity provided by different approaches to security is itself an element of that security. Establishing a technology-specific standard would provide a clear signal to criminals of where to focus their efforts.

The Proposed Issuer Standards

In addition to supporting the non-prescriptive approach to fraud prevention standards, Visa generally supports the language of the proposed standards in the Rule and the accompanying Commentary. In some cases, however, Visa believes that the language should be revised to address more fully the variety of factors that contribute to fraud in electronic debit transactions.

Identification

In the Commentary discussion of automated mechanisms to assess the risk that a particular electronic debit transaction is fraudulent, the Board provides an example of the use of neural networks to identify potential fraud. Visa believes that the Board should add a sentence to this portion of the Commentary to highlight that an issuer may want to review the effectiveness of the authorization rules that govern such automated mechanisms in order to ensure that these mechanisms are keeping pace with evolving fraud patterns.

In the discussion of authentication of the cardholder at the point of sale, Visa believes that the Board should recognize that authentication of the device that is used in an electronic debit transaction and the authentication of the person using the device are two separate issues that are often addressed by separate technologies or processes. For example, Visa believes that the Board should state that "an issuer may specify the use of particular technologies or methods to validate whether the payment device or cardholder is authorized to use the card at the time of the transaction."

In addition, Visa believes that the Board should expand the language on the assessment of the effectiveness of the different authentication methods to include an assessment of the acceptance channels as well. A full appreciation of the fraud rates associated with different methods of authentication requires a review of the acceptance channels, *e.g.*, card present v. card not present and domestic v. international. For example, practices to encourage the use of other means of authentication, as encouraged by this same Comment, require consideration of the extent to which a particular means of authentication is viable in a particular acceptance channel, as well as transaction amounts. For example, issuer fraud reporting indicates that there is no material difference in fraud rates between authentication methods for transactions less than $50, which have accounted for approximately 80 percent of all debit transactions.

Even if an issuer found that PIN transactions resulted in lower fraud rates than signature transactions overall, including consideration of ATM fraud losses due to the compromise on PIN numbers, encouraging PIN transactions would be of no benefit to the extent that the differing fraud rates were concentrated in card-not-present transactions where PINs generally are not used. Similarly, other references to authentication methods in that Comment should also refer to acceptance channel to ensure that issuers have a holistic view of the effectiveness of each authentication method, including for low and high value transactions. In addition Visa supports the language in this Comment that consideration of adopting new methods of authentication focus on whether use of such authentication methods is practical. New, robust means of

authentication that cardholders will not use, or that merchants will not accept, will not prevent fraud to any appreciable degree.

Monitoring

Visa supports the Board's proposal for a flexible standard for monitoring fraudulent electronic debit transactions, as it allows issuers latitude to track and analyze fraud and fraud-related trends, as appropriate, based on factors relevant to their individual portfolios, such as varying products, merchant environments, performance by transaction amount, and authentication method.

Responding to Fraud, Securing Data, and Annual Review

Visa supports the language of both the Rule and the Commentary relating to these subparagraphs.

Certification

Visa generally supports the language of both the Rule and the Commentary on the certification requirement. However, it is not clear how the fraud prevention standards will be enforced in practice and what the network role in that process will be. Visa assumes that adherence to the standards will become part of the regular bank examination process. If an issuer is found to be so deficient in meeting the standards that its eligibility to receive the fraud-prevention adjustment will be suspended by the appropriate federal banking agency, to avoid unnecessary changes in eligibility Visa believes that issuers should be given a period of between 90 and 180 days to come into compliance after a finding of a deficiency. In addition, Visa believes that networks will need at least 30-days advance notice to change the fraud-prevention adjustment treatment for individual issuers. Visa also believes that it is critical that either the networks be informed of required changes in eligibility for the fraud-prevention adjustment or that the 30-day period begins to run only after the networks have received notice from the issuer of a change in status.

* * * *

We appreciate the opportunity to comment on this important matter. If you have any questions concerning the issues raised in this letter, do not hesitate to contact me at (415) 932-2244.

Sincerely,

Joshua R. Floum/Dem

Joshua R. Floum
General Counsel