September 30, 2011

Ms. Jennifer J. Johnson
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, N.W.
Washington, D.C. 20551

Re: Interim Rule on Debit Card Fraud Prevention Adjustment, Docket No. R-1404

Dear Ms. Johnson:

Bank of America, N.A. ("Bank of America") appreciates the opportunity to comment on the interim final rule issued by the Board of Governors of the Federal Reserve System ("Board") allowing an issuer to receive an adjustment of one cent to its debit card interchange transaction fee if the issuer takes certain steps to monitor and prevent fraud losses ("interim final rule"). Bank of America is the leading debit card issuer in the country and has a deep understanding of the economic underpinnings of the debit card product, its functionality, and its appeal to consumers and merchants alike. In 2010, Bank of America's customers conducted more than 5.6 billion debit transactions on approximately 22 million debit cards representing approximately $240 billion in purchases. On an average day the Bank processed more than 15 million transactions (approximately 180 transactions a second), representing $658 million of consumer and small business spending.

Bank of America strongly supports the Board's interim final rule allowing issuers to receive an adjustment for anti-fraud measures. Bank of America devotes considerable resources to protect consumers from fraudulent transactions. It is imperative that issuers receive appropriate compensation from merchants to protect consumers from many fraud risks, including those presented by merchant data breaches. Without this compensation, consumers (and banks) could be harmed because issuers may be unable to provide the level of world-class fraud protection that consumers have come to expect. Furthermore, we believe that allowing such an adjustment will allow issuers to better recognize *legitimate* transactions, furthering the successful processing of payment transactions for consumers and merchants. Although we are pleased that the Board recognizes the need for an adjustment to the interchange amounts provided under Regulation II, we believe that the additional one cent per transaction allowed by the interim final rule is not adequate to cover the costs issuers incur in preventing fraud losses. We therefore urge the Board to increase the amount issuers may receive. Additionally, we respond to the Board's request for feedback on the relative security of different authentication-type transactions, which we believe is an important area of consideration.

We also support the Board's proposed approach to fraud prevention requirements applicable to card issuers, including a non-prescriptive approach to certification. We strongly believe that such an approach promotes a market-driven, threat-responsive, and nimble operating environment that can best protect customers from fraudulent activity. We believe that the Board should ensure that this approach does not adversely affect the incentives for avoiding fraud that exist under well-established network rules that apportion liability to the party in the best position to avoid fraud losses.

Fraud Prevention

Consumers demand safe and secure methods, including debit cards, to make their payments. Bank of America devotes significant resources to providing a debit card that consumers can use with confidence. This is a constantly evolving area of focus, and new risks continually emerge. These risks can be as obvious as large-scale merchant data breaches or as subtle as PIN-skimming from a merchant card reader. Bank of America works tirelessly to protect consumers from these types of risks.

The Board and consumers are well aware of many of the benefits that Bank of America provides to consumers in the form of fraud prevention, detection, and remediation. For example, Bank of America employs a robust transaction monitoring program to prevent and detect fraud. Bank of America also provides consumers with zero liability protection with respect to fraudulent debit card transactions, a benefit that goes beyond federal requirements.

What is perhaps less obvious is how our fraud prevention efforts enhance the overall customer and merchant debit card experience, allowing more transactions to be processed – to the benefit of issuers, customers and merchants. Fraud prevention efforts of issuers eliminate a significant portion of total fraud exposure each year. If these transactions were not prevented, customers would experience more fraud, have less confidence in the system, and use their cards less frequently. Also, the additional fraud would result in the cancellation and reissuance of more cards, denying customers the choice to use their debit cards. This could result in consumers using less convenient methods of payments for merchants. Finally, issuers' ability to learn from their customers' patterns of use allows them to identify with particularity true fraud and process most legitimate transactions. The result is that issuers can process more transactions with less disruption to customers and merchants.

We appreciate the Board's recognition of the importance of fraud prevention programs, a key component of a successful fraud risk management process. Implementation of preventative measures leads to greater success managing fraud risk than relying solely on detection and recovery processes. As noted in the premise for allowing five basis points of transaction value as compensation for fraud losses, it is important that all participants in the electronic debit payment system (including merchants, merchant-acquirers, networks and issuers) focus on fraud prevention. A high level of fraud protection instills customer trust in the payment system and encourages the entire system's sustainability.

The Board appropriately focused on the estimated fraud prevention costs expended by different parties and concluded that the median amount spent by issuers on all reported fraud-prevention activities was approximately 1.8 cents per transaction. First, we believe that the Board should use the cost for issuers at the 80th percentile, rather than issuers' median costs. This would be consistent with the approach taken by the Board when setting the cap for interchange. Second, not all fraud-prevention costs spent by issuers were factored into the calculation of the 1.8 cent figure, which is what determined the one-cent-per-transaction value set in the interim final rule. Set out below are descriptions of important activities on which issuers spend more than they would recover with a one-cent-per-transaction adjustment. These higher costs should be factored into the adjustment, in order to encourage the continued investment that prevents fraud for merchants, issuers, and customers. In particular, we urge the Board to include the costs of customer support in fraud prevention costs. In three other important areas -- research and development, consideration of the full fraud costs that result from PIN compromises, and the compromise of debit card account numbers -- we believe that issuers incur costs beyond those that were considered by the Board. Including the full range of these fraud prevention costs would recognize the higher costs issuers spend on fraud prevention.

- **Customer Support.** Cardholders themselves are the best monitors and guardians of the money in their checking accounts. As an issuer, Bank of America provides around-the-clock service and support to our customers. Many customer inquiries relate to questionable account transactions that aid in the detection of fraud and prevention of additional fraudulent activities. Bank of America customers who have any questions about the validity of a transaction affecting their accounts have access 24 hours a day, seven days a week to customer service representatives who are trained in fraud prevention and questionable billing activity response. We have invested in multiple channel formats to enable our customers to select the most convenient and immediate customer service channels for their use. Channels include physical bank branches, toll-free customer service numbers, online web service, and online chat for customer service.

While ensuring multiple access channels at anytime requires heavy investment, it is a crucial component of preventing and protecting customers from fraud. It allows us to gather information about lost and stolen cards reported by customers, so that those cards can be cancelled. This prevents further fraudulent use of the cards, reducing merchant and issuer exposure to fraud, and limiting the time and expense merchants might otherwise spend addressing customer concerns. For example, a customer who notices an unusual transaction made at a big-box retailer will call the guardian of his funds -- the bank associated with his account -- rather than customer service at the retailer where the transaction occurred. We also provide payment transaction clarity by deciphering merchant identities and transaction amounts to prevent unwarranted charge backs for unauthorized transactions and expenses for merchants. These activities are services that assist both customers and merchants.

- **Research and Development.** As an issuer, Bank of America invests heavily to keep up with the changing nature of payment methods and to minimize potential vulnerabilities due to emerging fraud. As the Board noted, the fraud environment is never static. What can effectively and efficiently prevent fraud today will be challenged tomorrow, as new payment mechanisms are developed. For example, in recent years, online and mobile banking have gained popularity, adding both convenience for customers as well as new opportunities for fraudsters. These opportunities will continue to change, as newer ways to access accounts are developed – including Person to Person and new debit and prepaid products. For issuers, investment in R&D is a prerequisite for reducing fraud losses. Under the proposed interim final rule, all fraud technology costs would be considered part of the one-cent allowance. We believe that this decision will reduce the economic viability of continuing the R&D investment levels issuers employ today to mitigate the risks that they must assume. Ultimately, this may result in less effective fraud prevention capabilities, compromising the safety of customers' funds and increasing fraud exposure for issuers and merchants.

- **True PIN-loss Rate.** Thirty percent of losses from all PIN transactions (including point of sale and at ATM) are due to merchant data breaches, resulting in approximately $500 million in claims and $50 million in operating expense across the industry annually. When debit card data and PIN information are compromised as a result of merchant breaches, losses aren't limited to retail transactions; experience shows that there will be increased fraudulent ATM transactions involving the compromised PINs. When debit card numbers and PINs are stolen, fraudsters find it more lucrative to use ATMs to withdraw cash, rather than making retail purchases.

Including these ATM transactions in the loss rate for PIN-authenticated POS transactions more than doubles those losses, significantly reducing the apparent security advantage of PIN over signature. Thus, while we understand that it may appear that PIN transactions are more secure than signature transactions, this conclusion changes when all debit losses related to PIN compromises (and not just those incurred at point of sale) are considered. Consequently, we caution the Board that it should not consider PIN to be an inherently lower risk authorization type. It is vulnerable to the same risks presented by all static data elements in the payments system today.

- **Debit Card Account Number Compromise.** Issuers incur significant expenses as a result of merchant data breaches involving debit card data. Issuers must make significant investments to perform critical fraud-prevention analyses of their card portfolios in response to compromised card data. For example, in order to minimize payment disruptions to customers, issuers will undertake intensive account portfolio review, analyzing the extent of portfolio compromise and the account-level risk of fraud, in order to minimize payment disruptions to customers. Once card numbers are identified as having elevated risk of being compromised, issuers proactively monitor the accounts, typically incurring expenses communicating to the customers affected and responding to inquiries from the customers. This fraud analysis requires a heavy initial investment, but it also serves to identify, prevent or limit subsequent fraud losses on those accounts that are most at risk. For those accounts, issuers often incur additional direct expenses in re-issuing compromised accounts, which involves card production and mailing, servicing impacted customers, and designing and implementing prevention programs specific to the compromise. Furthermore, when issuers proactively take compromised cards out of circulation (which they frequently do in response to a compromise), they not only incur operating expense, but also may lose revenue during the periods that customers are not able to use their debit cards. These actions, taken by issuers at their expense, protect both consumers and merchants from fraud losses.

Not all the costs outlined above were factored into the Board's one-cent fraud adjustment. Specifically, the Board did not include the costs of customer support and responding to customer inquiries concerning fraud, which can be significant. When these are included in issuers' costs, along with the full range of costs incurred by issuers in the other categories listed above, it is clear that issuers currently spend more than one cent per transaction on anti-fraud measures. Issuers should have economic incentive to continue these efforts, which benefit merchants, customers and themselves. Therefore, we urge the Board to consider these additional costs when setting the final fraud prevention adjustment, which we believe should be based on the costs of issuers at the 80th percentile, not those at the median.

As the Board pointed out, the fraud-prevention adjustment to the interchange transaction fee is effectively paid by merchants to issuers. It is appropriate for the merchants to contribute their fair share toward the costs of preventing fraud in the system. As stated above, issuers' anti-fraud efforts prevent a significant portion of attempted fraud, resulting in fewer claims ever being asserted to merchants. Importantly, the elimination of such a significant portion of fraud risk from the system results in a more robust, effective and trusted system, allowing more debit card transactions to be processed. This benefits all system participants, including merchants.

Additionally, as noted above, a significant portion of losses related to PIN compromises result from merchant security breaches. These losses, as well as costs of cancelling and reissuing cards and otherwise "cleaning up" these problems, fall on issuers. It is fair for merchants to help defray these costs, by allowing issuers to recover more for the fraud adjustment.

Certification

The interim final rule does not prescribe the particular anti-fraud measures that an issuer must take. This non-prescriptive approach will allow issuers to continue to focus on research and development of new authentication, prevention and detection methods and tools to stay ahead of evolving fraud. As the Board stated, "the dynamic nature of the debit card fraud environment requires standards that permit issuers to determine themselves the best methods to detect, prevent, and mitigate fraud losses for the size and scope of their debit card program and to respond to frequent changes in fraud patterns." These changes will vary from issuer to issuer, depending on the makeup of each debit card program and the customers involved. We strongly believe that this non-prescriptive approach promotes a market-driven, threat-responsive, and nimble operating environment that can best protect customers from fraudulent activity by allowing each issuer to determine how to best identify and quickly respond to new threats of fraud targeting its customers.

Bank of America also commends the Board on the certification process outlined in the interim final rule. The proposed certification process encompasses the key elements of a sound fraud prevention program: Issuers will be eligible for the fraud prevention allowance provided they certify their compliance on an annual basis with the Board's fraud-prevention standards to the payment card networks in which they participate. Network-approved certification requires an annual review of fraud prevention policies and procedures with a component calling for more frequent review should a significant event occur.

However, we urge the Board to ensure that this approach does not adversely affect the incentives for avoiding fraud that exist under well-established network rules. These rules apportion liability to the party in the best position to avoid fraud losses. For example, we are concerned that the Board's statement "that an issuer's policies and procedures do not provide an appropriate response if they *merely* shift the loss to another party, other than the party that committed the fraud" (emphasis added) might be misconstrued.

We note that the current system balances risks and rewards among all participants. Current network rules provide incentives for issuers and merchants to invest in fraud technology tools. A party that fails to implement available solutions to prevent and detect fraudulent activity may assume the risk of loss of the transactions that it could have prevented. By providing incentives and guidance on tools that can be used to avoid potential losses, the network rules do much more than *merely* shift liability. In addition to implementing and enforcing these rules, networks also continuously reevaluate them, resulting in updated practices that protect consumers. We encourage the Board to support the maintenance of the current payment network rules system.

Conclusion

We agree with the Board on the importance of fraud prevention to all payments system participants. While we support the Board's interim final rule allowing issuers to receive an adjustment for anti-fraud measures, the amount of the fraud adjustment is not adequate to cover issuers' true costs incurred in providing anti-fraud services. We believe that all issuers must be assured they will receive just compensation for their investments and urge the Board to increase the fraud adjustment to cover those costs. Additionally, we strongly support the Board's non-prescriptive approach to certification. We firmly believe that the best way to protect our customers and their funds is through this non-prescriptive approach that allows flexibility to adjust operations to prevent and quickly respond to ever-changing fraud threats.

Thank you for the opportunity to share our views. We would be pleased to discuss any of them further at your convenience.

Sincerely,

Mark K. Metz

Mark K. Metz
Deputy General Counsel