Tom Brooks
Executive Vice President
Cards and Payments Executive
Consumer Services Group

REGIONS

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

RE: Interim Final Rule: Debit Card Interchange Fee and Routing – Docket No. R-1404 and RIN No. 7100 AD63 Response to the Board's Requests for Comments by Regions Bank

Dear Ms. Johnson:

Regions Bank[1] has broad experience in the debit card business. It is the sixth largest debit card issuer based on transaction volume. Our customers carry over 4 million debit cards and last year alone, they engaged in in over 700 million debit card transactions.

Therefore, Regions appreciates the opportunity to comment on the interim final rule adopted by the Federal Reserve Board that governs adjustments to debit interchange transaction fees for fraud-prevention costs (the "Interim Rule").

The Interim Rule is a proposal to implement Section 920(a)(5) of the Electronic Fund Transfer Act ("EFTA") that permits the Board to adjust the reasonable interchange transaction fees that an issuer may receive to allow for the costs incurred by the issuer in its fraud-prevention efforts. In Section 920(a)(5), Congress requires the Board to "prescribe regulations . . . to establish standards for making adjustments" to the interchange fees that may allow an issuer to recoup its costs for its fraud-prevention activities if it complies with the fraud-related standards established by the Board.

This mandate is recognition of the threat that fraud in all its manifestations poses to the debit payment system and the increasingly sophisticated attacks by fraudsters to

---

[1]Regions Bank is a wholly-owned subsidiary of Regions Financial Corporation, with $132 billion in assets, is a member of the S&P 100 Index, and is one of the nation's largest full-service providers of consumer and commercial banking, trust, securities brokerage, mortgage and insurance products and services. Regions serves customers in 16 states across the South, Midwest and Texas, and through its subsidiary, Regions Bank, operates approximately 1,800 banking offices and 2,200 ATMS. Additional information about Regions and its products and services can be found at www.regions.com.

break down payment system defenses wherever they find system vulnerabilities – at all levels of and parties to the payment system. Fraud protection is one of the key factors that differentiates debit card transactions from check transactions. It contributes to the convenience and security of each debit card transaction and provides a key benefit that both customers and merchants have come to expect.

Section 920(a)(5) also reflects the critical role of issuing banks in detecting, preventing, and mitigating fraud as it arises and the fact that, as the Board recognizes, the issuing banks cover the vast majority of fraud losses, whether measured in number of transactions or total dollar value.[2] Indeed, consumers bear virtually no out-of-pocket loss for fraudulent activity.[3]

We agree with the Board's Interim Rule that adopts flexible, non-prescriptive fraud-prevention standards for issuers who seek a fraud-prevention adjustment. As the Board recognizes, there are many advantages to the proposed rule over an alternative that would have limited a fraud-prevention allowance to the use of particular technologies specified by the Board. Among other things, the Board's approach will allow issuers to use fraud-prevention measures that best suit their businesses, to adopt new and varied methods and technologies to combat fraud, and to be able to respond quickly and flexibly to new methods employed by criminals. The Interim Rule also properly requires issuers to review its fraud-prevention policies and procedures to ensure their continued effectiveness in the changing landscape of fraudulent activity.

In addition, we believe the Board was correct in applying the allowance to both signature and PIN debit card transactions. The purpose of the allowance is to encourage issuers to take measures to prevent fraud irrespective of debit card type. There is no real benefit to consumers, merchants or the system itself to discourage investment and activities to prevent fraud in one type of debit card transaction over another.

Further, we agree with the Board that without adequate funding issuers' fraud-prevention activities could be reduced and that in keeping with Congress's direction in Section 920(a)(5), a fraud-prevention allowance is entirely appropriate. In its Interim Rule, the Board set a cap of 1.0¢ as an allowance for the cost of an issuer's fraud-prevention activities provided that the issuer certifies its compliance with the Board's anti-fraud requirements.[4] In light of the statute's factors and the other appropriate factors the Board considered and the ultimate goal to have issuers engage in robust, innovative, flexible, and cost effective anti-fraud measures, Regions respectfully requests that the Board consider:

1. Whether the fraud-prevention allowance should be the same amount for all transactions or should be a percentage of the value of each transaction.

---

[2] 76 Fed. Reg. 43481 (July 20, 2011) and 76 Fed. Reg. 43397 (July 20, 2011).
[3] 76 Fed. Reg. 43481 (July 20, 2011)
[4] Section 235.4.

2. Whether fraud-prevention policy would better be served if the fraud-prevention allowance to qualified issuers corresponded to (a) the fraud-prevention costs of the typical user [2.9¢] or (b) the costs of the substantial majority of covered issuers corresponding to average the 80th percentile issuer's average per-transaction costs [3.1¢] (the measure used for interchange fees) as opposed to the Interim Rule's measure of the average of the fraud prevention costs for all fraud prevention transactions which weighs the results heavily toward the low costs of 3 large issuers responsible for over half of all debit transactions [1.8¢]. [5]

3. Whether the fraud-prevention allowance should be a cap as the Board proposes or a required adjustment for issuers who satisfy and certify that they have met the Board's anti-fraud requirements, with additional flexible adjustments to encourage innovation and to account for market changes and merchants' fraud-prevention engagement.

4. Whether the fraud-prevention allowance should be adjusted to account for (a) issuers who engage in significant additional expenditures to enhance their anti-fraud systems, such as adding EMV contact and contactless chip technology and/or (b) increased fraudulent activity.

5. Whether merchants who fail to comply with PCI-DSS anti-fraud standards should be required to pay interchange fees without a regulatory cap or higher interchange fees to encourage merchants' participation in anti-fraud prevention and to level the playing field between merchants and issuers for anti-fraud activity and costs.

I. A Reasonable Fraud-Prevention Adjustment for Issuers Should Be Based on the Post-Regulation Environment and Should Encourage Issuers to Engage in Fraud-Prevention Activities

The Board is correct in its observation that Section 920(a)(5) of the EFTA does not specify the amount or the range of amounts that is "reasonably necessary to make allowance for" the costs incurred by issuers in their fraud-prevention activities[6] nor is the Board statutorily *required* to provide an adjustment that fully compensates issuers for their fraud-prevention costs. However, fraud-prevention and issuers' central role in fraud-prevention should be given special consideration because of their importance to consumers, merchants, and the entire debit payment system.

---

[5] 2009 Interchange Revenue, Covered Issuer Cost, and Covered Issuer and Merchant Fraud Loss Related to Debit Card Transactions, June 2011 (the "Survey") p. 16, Table 13 p. 30. The proposed fraud adjustment in § 235.4 is 1¢ because 0.7¢ per transaction monitoring costs were included in the interchange fee cap. *See* 76 Fed. Reg. 43482-43483 (July 20, 2011).

[6] 76 Fed. Reg. 43482 (July 20, 2011)

Moreover, the determination of the amount "reasonably necessary" to make allowance for issuers' fraud-prevention costs should take into account the effects of the final regulations under Section 920 that replaces market-determined interchange fees (which averaged out to 44¢ per transaction)[7] to an imposed cap for each transaction of 21¢ and 5 basis points multiplied by the value of the transaction.[8] Because it is a cap rather than a set fee, the full extent of this massive reduction of the issuers' interchange fees is yet to be seen.

This huge loss of the issuing banks' compensation directly related to their debit payment services is directly relevant to the issuing banks' fraud-prevention activities. As the Board recognized, the pre-regulation interchange fees dictated by the market "may have allowed issuers to offset both their fraud losses and fraud-prevention costs and fund innovation on fraud-prevention tools and activities."[9]

The Board's post-regulation artificial cap on interchange fees will starve issuers for funds for their debit payment system and many issuers will lose money on each transaction. This necessarily will remove funds that would have been earmarked for fraud-prevention and innovation. Moreover, it will reduce significantly issuers' incentive to direct funds for innovation in a business sector that will no longer be profitable for many banks. This is just market reality.

In discussing the basis for its fraud-prevention adjustment, the Board opines that "[i]ssuers have a strong incentive to protect cardholders and reduce fraud independent of interchange fees received."[10] The sole reason the Board gives for this presumption is that "[c]ompetition for cardholders suggests that protecting their cardholders from fraud is good business practice for issuers."[11] This rationale may have been true in pre-cap days when issuers profited from their debit card payment services and offered rewards and free checking to their cardholders. But those days are, or very shortly will be, ended. There will be very little competition for business that has been administratively designed to be break even and, in fact, will cause losses for many issuers.

The Board has recognized the inherent danger of a failure to adequately compensate issuers for their fraud-prevention and data security activities.

> Without adequate funding, fraud-prevention activities could be reduced, thereby causing harm to consumers, merchants, and issuers.[12]

---

[7] 76 Fed. Reg. 43397 (July 20, 2011)
[8] § 235.3
[9] 76 Fed. Reg. 43481 (July 20, 2011)
[10] *Id.*
[11] *Id.*
[12] 76 Fed. Reg. 43486 (July 20, 2011)

Accordingly, the standard for adjustment for issuers' fraud-prevention activities should (a) compensate issuers to maintain their fraud-prevention activities commensurate with their ongoing activities, (b) encourage innovation, flexibility and investment by issuers in fraud prevention activities, and (c) encourage merchants' participation in fraud-prevention.

The Board's 1.0¢ cap on an adjustment for issuers' fraud-prevention activities does not reasonably address these goals nor the Board's more fundamental role to protect the integrity of financial institutions, the financial sector, and the public.

II. The Reasonable Allowance for Fraud-Prevention Should Be Based on the Fraud-prevention Costs of Most Issuers and the Value of the Transaction

a. The Fraud-Prevention Adjustment Should Be a Percentage of the Total Value of a Transaction

We believe that the amount of the fraud adjustment should not be a set amount for all transactions, but rather should be a percentage of the total value of each transaction. This would more properly allocate the per transaction cost of fraud proportionately to the value of the transaction. Otherwise, a fixed amount would unfairly burden lower value transactions with the cost of fraud-prevention represented by higher value transactions. This ad valorem approach would be consistent with the Board's adoption in the final interchange fee standard of an ad valorem component for fraud losses that corresponded to the average per-transaction fraud losses of the median issuer.[13] As with fraud-prevention losses, an ad valorem fraud-prevention adjustment would reflect the variation in transaction costs based on the value of the transaction.

b. The Appropriate Fraud-Prevention Adjustment Should Correspond to the Typical Issuers' Fraud-Prevention Costs of 2.9¢

The Board based the set amount of 1.0¢ per transaction[14] for the fraud-prevention adjustment on the median fraud-prevention costs[15] of all issuers responding to the Board's 2009 Survey which were 1.8¢ per transaction.[16] The Board's use of a medium of all the transaction costs of the issuer respondents does not fairly or reasonably represent typical issuer's fraud-prevention costs per transaction.

This becomes readily apparent when you consider that over 55% of the total volume of debit transactions in the United States is represented by only 3 high volume

---

[13] 76 Fed. Reg. 43422 (July 20, 2011)

[14] The actual per transaction fraud-cost allowance is 1.8¢ rounded down to the nearest cent to account for the 0.7¢ transaction monitoring costs that were a part of the interchange standards. 76 Fed. Reg. 43483 (July 20, 2011).

[15] 76 Fed. Reg. 43479 (July 20, 2011)

[16] The proposed fraud adjustment in § 235.4 is 1¢ because 0.7¢ per transaction monitoring costs were included in the interchange fee cap. *See* 76 Fed. Reg. 43482-43483 (July 20, 2011).

issuers – Bank of America (22.5%), Wells Fargo (18.0%) and Chase (14.8%).[17][18] As a result, over half of the fraud-prevention costs considered in determining a simple average per transaction cost are those of the three dominant issuers.

These big three issuers' cost structures for fraud-prevention with their enormous economies of scale obviously do not represent the average per transaction fraud-prevention cost structures of the typical issuer – either those of the other 63 respondents whose results were used in the Board's Survey or those of the 12,330 debit card issuers in the United States who were not surveyed. Using the Board's current method of computation of cost essentially requires the typical issuer to have its fraud-prevention costs comparable to the costs of the top three issuers with their economies of scale and who dominate the overall market. This is not a reasonable or wise outcome to encourage issuers to engage in pro-active and robust fraud-prevention, but this, in fact, is the result of the method of cost calculation adopted for the proposed Interim Rule.

The statute clearly indicates that the fraud-prevention allowance should be based on the issuer's costs. Specifically, Section 920(a)(5)(a)(i) provides that the adjustment should be "reasonably necessary to make allowance for costs incurred *by the issuer*." (emphasis added). While practicalities may prohibit allowances determined by each individual issuer's fraud-prevention costs,[19] the fraud-prevention allowance should be based on the costs of the typical issuer.

This approach fits with the policy and purpose of the allowance permitted by Section 920(a)(5) to encourage the mitigation of fraud through the efforts of all issuers, not just three, and thereby to aid consumers and merchants and to strengthen the payment system.

The Survey shows that the mean fraud-prevention costs per respondent are 2.9¢ per transaction.[20] Such a measure more closely approximates the reality of an issuer's costs and therefore more reasonably and fairly compensates an issuer for its fraud-prevention activities that are in everyone's interests. This amount does not compensate all issuers for all their fraud-prevention costs. It still imposes cost discipline on all issuers whose cost fall below those of the mean issuers.

This suggested approach comports with the Board's approach in determining the appropriate interchange fees in its final rule. There, the Board determined that the appropriate interchange fee standard should be "reasonable or proportional to the overall

---

[17] Nielsen Report, Issue 90 April 2011

[18] After Chase, the percentage of the issuers' percentage of debit purchase volume falls precipitously. US Bank, the fourth ranked issuer, only has 3.8% of purchase volume and Regions, the sixth largest issuer, only has a 2.5% of purchase volume (about a tenth of Bank of America's volume).

[19] 76 Fed. Reg. 43422 (July 20, 2011)

[20] Survey, p. 16, Table 13 p. 30. "The mean per respondent is the average of each respondent's ratio of reported costs for a particular category to its purchase transactions."

cost experience of the substantial majority of covered issuers."[21] Similarly here, the Survey's mean fraud-prevention cost per respondent of 2.9¢ would represent the experience of the majority of covered issuers and not be skewed to the unrepresentative few. Therefore, Regions believes that the appropriate fraud-prevention adjustment should be a fixed amount of 2.9¢ per transaction or an ad valorem amount corresponding to the Survey's mean fraud-prevention cost per respondent of 2.9¢.

c. The Consistent Measure Would Be the Overall Cost Experience of the Substantial Majority of Issuers -- the 80th Percentile Issuers' Average Fraud-Prevention Costs of 3.1¢

To obtain a standard that was reasonable or proportional to the overall cost experience of the substantial majority of covered issuers, the Board used a standard that corresponds to the 80th percentile issuer's average per-transaction costs.[22] Therefore, if the Board were consistent in its method of determining a fraud-prevention standard as its method of determining the standard for an interchange fee, it would use a standard that corresponds to the 80th percentile issuer's average per-transaction fraud-prevention costs of 3.1¢ either as a fixed amount or a corresponding ad valorem adjustment.[23]

d. The Board Should Consider Additional Fraud-Prevention Costs in the Future

Even an additional fixed or ad valorem allowance corresponding to the mean fraud-prevention costs per respondent of 2.2¢ (2.9¢ minus the already included 0.7¢) would not fully compensate issuers for issuer's fraud-prevention activities. The Board has chosen to ignore various generally accepted activities that issuers use to mitigate or prevent fraud. For example, "the Board has not included the costs of cardholder inquiries in establishing the fee standard."[24]

But, handling customer inquiries and taking appropriate action concerning fraud or possible fraud is an important and well recognized part of fraud mitigation. The recent security breach of the retailer Michaels Stores, Inc. arising from PIN pad tampering[25] illustrates the central importance of issuing banks and their customer service when a breach occurs. When Michaels first emailed its customers on May 6, 2011, to inform

---

[21] 76 Fed. Reg. 43433(July 20, 2011)
[22] 76 Fed. Reg. 43433-34 (July 20, 2011)
[23] Survey, Table 13 p. 30.
[24] 76 Fed. Reg. 43429 (July 20, 2011)
[25] Gregory Karp and Amy Alderman, *Michaels Customers Fall Victim to Debit Card Thefts,* Chicago Tribune, May 5, 2011, http://articles.chicagotribune.com/2011-05-05/business/ct-biz-0506-michaels-20110505_1_debit-card-swipe-pin-pads and Ann Zimmerman and Miguel Bustillo, *Thieves Swipe Debit Card Data,* The Wall Street Journal, http://online.wsj.com/article/SB10001424052748703730804576319033369439712.html

them that their credit and debit card information might be compromised, it advised them to contact their banks.

> We recommend immediately contacting your bank and/or credit card company to check for and report any unauthorized charges, as well as seek their advice on how to protect your account in the event that your information has been taken.[26]

Michaels did not at that time set up a help line or contact number to address customer inquiries. Instead, customers were sent to the banks' call centers. The banks then were required to deal with the effects of the merchant's security breach and the associated costs – responding to customers' inquiries, sending out alerts to its customers, setting up new accounts, and issuing new cards. Even in its subsequent May 2011 press release, Michaels urged its customers who found suspicious activity to contact their bank issuer: "Customers who believe their accounts were used without authorization should contact the card issuer directly."[27]

We urge the Board to include in its next survey cycle the amount of costs that issuers expend in handling customer' fraud inquiries, notifying customers generally of fraud breaches of merchants and others, and similar fraud-prevention activities. Such additional information from issuers will better inform the Board in its future allocation of the fraud-prevention costs of issuers.

Issuing new cards is another anti-fraud measure that is not calculated in the reasonable compensation of issuers.[28] However, new debit cards come with new CVV codes that diminish the amount of fraud for non-card present transactions where the greatest amount of fraudulent activity takes place. It costs an issuer approximately $1 per card for a replacement.

III. The Fraud-Prevention Allowance Should Be a Required Adjustment to the Interchange Fee, Not a Cap

Because of the special place fraud-prevention has to help ensure the integrity of the debit payment system and issuers' key role in fraud-prevention, the allowance for fraud-prevention should not set the maximum allowable adjustment, but, instead, should

---

[26] Email dated May 6, 2011, from John Menzer, CEO of Michaels Stores, Inc. to Michaels customers, (May 6, 2011), available at http://consumerist.com/2011/05/michaels-warns-customers-of-possible-data-breach.html

[27] Michaels May 2011 Press Release "Michaels Shares New Information in PIN Pad Tampering Investigation", available at http://www.michaels.com/Press-Releases/Press-Releases,default,pg.html.

[28] 76 Fed. Reg. 43428 (July 20, 2011)

be a required adjustment for issuers who meet the Board's fraud-prevention requirements along with additional increases depending on additional factors to spur fraud-prevention.

Under the Board's new system, the future competition among networks will be for merchants, not issuers. Concomitant with this network competition will be their willingness to negotiate away the interchange fees due to issuers by big merchants. Interchange fees paid by big volume retailers are already well-below the cap that will be imposed by the Board. With their ever-increasing clout, big merchants have begun to demand even lower interchange rates from networks who are anxious for their business and whose competitive need to keep issuers satisfied has greatly diminished. A fraud-prevention adjustment is not something that should be a negotiating football for the networks and the big merchants.

There is no statutory requirement to set a cap on fees; after all, the act merely requires the Board to set standards. A required adjustment for fraud-prevention would fit in well with the statutory framework to reasonably compensate issuers for their fraud-prevention costs. It does not make sense to have those fees diminished based on negotiations that have nothing to do with fraud-prevention or data security. Moreover, any additional cuts in the fees to issuers would further discourage their efforts to engage in anti-fraud activities beyond those required by the Board and other governmental authorities, by statute, and by industry standards.

IV. The Board Should Allow for Incremental Adjustments for Issuer Anti-Fraud Investment and for Significant Increases in Fraudulent Activities

A. Innovation and Investment in Fraud-Prevention and Data Security Measures Should Be Encouraged

The fraud-prevention adjustment cap in the Interim Rule reflects a zero innovation policy. The Interim Rule is based on the per transaction average of fraud-prevention costs two years ago and has no flexibility that would encourage innovation and anti-fraud investment. As the debit payment delivery systems become more diverse with debit cards morphing into mobile communication devices and electronic keys and electronic information becoming more of a target of increasingly sophisticated criminal organizations across the world, issuers should be encouraged to invest and innovate to increasingly greater degrees in means to prevent fraud, to mitigate its effect, and to secure electronic data.

Advances in technology that would lessen fraud continue to present themselves to issuers. For example, EMV technology[29] which has not been widely adopted in the United States would be a useful anti-fraud tool. Issuer adoption of this technology would

[29].EMV stands for Europay, MasterCard and VISA, a global standard for inter-operation of integrated circuit cards (IC cards or "chip cards") and IC card capable point of sale (POS) terminals and automated teller machines (ATMs), for authenticating credit and debit card transactions.

require massive effort and expense. For example, Regions has received an estimate from an industry expert that the cost of issuing EMV cards would be $3.50 for each of Regions' 4,000,000 cards. But, an unreasonably low level of a capped allowance for anti-fraud activities will provide very little money or incentive for issuing banks to invest in such technology.

The Board should adopt a final rule that permits an adjustment on top of a fixed minimum fee to allow for investment by issuers in new technologies or other anti-fraud or data security activities that have a reasonable likelihood of mitigating fraud or improving the security of data. This adjustment could provide all or a portion of the issuers' investment on a per transaction basis and could be administered by the networks.

B. Increased Fraudulent Activity

The Board's determination of a reasonable allowance for issuers was based on one survey covering a single year – 2009. The report from that survey estimates that the median loss per transaction for issuers alone was 2¢, more than twice the cost to merchants, the only other party to a debit card transaction that suffers loss by fraud.[30] There is a no indication that the fraudulent activity for 2009 applicable to debit cards transactions was representative of past years or would be representative of the fraudulent activity three years later for 2012 -- the first calendar year that the new interchange calculations take effect – or beyond. Indications and common sense tell us, that, assuming debit card use continues to rise and thieves continue to become more sophisticated in their attacks on the debit payment system, the cost of fraud on a per transaction basis will likely increase as will the costs to issuers to counter such fraud. Moreover, the Board's new regulations will cause an increased migration to PIN-based debit card transactions. This in turn will increase the use, the availability, and the attractiveness of PIN numbers to thieves. As a result, there will be a significant increase of the theft of PIN numbers through phishing, vishing and other means, known and unknown. Thieves will use these cardholder PIN numbers to steal cash from issuers' ATM networks – further harming issuers. These ATM losses caused by compromised PIN debit cards were not considered in the determination of issuers' interchange fee standards in the Final Rules.[31]

If fraudulent activity significantly increases, the losses caused by such activity, particularly the disproportionate costs to issuers will increase – both in terms of the actual losses to issuers and the increased costs of fraud-prevention and mitigation. To allay somewhat these issuers' costs and to encourage issuers to increase their fraud-prevention and mitigation, Regions recommends that standards for a reasonable adjustment for fraud-prevention should be flexible. If fraudulent activity losses increase, issuers' should receive an additional adjustment to their interchange fees of one basis point for every two

---

[30] 76 Fed. Reg. 43397 (July 20, 2011). The total cost per transaction was 3¢; 76 Fed. Reg. 4381 (July 20, 2011)

[31] 76 Fed. Reg. 43433 (July 10, 2011)

basis points above 9 basis points, the current median fraud loss as a percent of transaction value.[32]

V. Issuers' Interchange Fees Should Be Adjusted for Merchants' Failure to Comply with Fraud Security Standards

The Board apparently based its determination of the appropriate fraud-prevention adjustment, in part, upon the assumption that merchants who participate in payment card systems are compliant with the PCI-DSS security standards. The Board states:

> In addition to these investments [anecdotal anti-fraud activities of some "large online merchants"], merchants also take steps to secure data and comply with Payment Card Industry Data Security Standards (PCI-DSS).[33]

However, in fact, merchant compliance with the PCI-DSS security standards is sorely lacking. The Visa chart "U.S. PCI DSS Compliance Status" shows that for the vast majority of merchants accounting for about a third of all Visa card transactions compliance to PCI-DSS standards is only "moderate among stand-alone terminal merchants, but lower among merchants using integrated payment applications."[34] The Board notes in its Interim Rule that even a merchant commenter recognized that different merchants represent different levels of risk and that it would be appropriate for interchange fees to be adjusted based "on the riskiness of particular merchants."[35] A merchant who fails to comply with the basic PCI-DSS security standards for its class obviously represents an increased risk to issuers and should pay for the increased risk that it causes.

As the Board's findings attest, it is the issuers who bear the brunt of fraud loss and have the primary day-to-day responsibility for anti-fraud activities. Merchants' lack of fraud-prevention and data security has severe impact on issuers. This has been demonstrated on a large scale by the widely publicized data security breaches this year with Sony that compromised the personal data including debit and credit card numbers, of over a 100 million consumers[36] and the Michaels craft store security breach that I referred to earlier. On a smaller scale, issuing banks encounter the effects of merchant

---

[32] 76 Fed. Reg. 43397 (July 10, 2011)

[33] 76 Fed. Reg. 43481 and *See* 43481 fn. 18 (July 10, 2011)

[34] *See,* "U.S. PCI DSS Compliance Status" located at http://usa.visa.com/download/merchants/cisp_pcidss_compliancestats.pdf.

[35] 76 Fed. Reg. 43483 (July 10, 2011)

[36] *Sony Data Breach: 100m Reasons to Beef Up Security.* ComputerWeekly.com, (May 3, 2011) available at http://www.computerweekly.com/Articles/2011/05/03/246559/Sony-data-breach-100m-reasons-to-beef-up-security.htm and Liana Baker, *Sony suffers Second Major User Data Theft,* (May 2, 2011) Reuters, available at http://www.reuters.com/article/2011/05/02/us-sony-idUSTRE73R0Q320110502.

security breaches every day and every day pay for these breaches with losses and additional costs.

Accordingly, we believe that merchants who do not comply with the PCI-DSS security standards by certification and validation, should not have their interchange fees capped and the reasonable interchange fees for these merchants should be the rates set by the market, not dictated by regulation. At the very least, the interchange rates for non-complying merchants should be increased to 6¢ per transaction (which is equal to issuers' fraud losses at an average of 3¢ per transaction and their fraud-prevention costs at an average of 3¢ per transaction) or an equivalent ad valorem adjustment.

The networks should determine the merchants who are not compliant with the PCI-DSS security standards on an annual basis. Further, the networks should manage and collect any increased interchange fees for non-complying merchants. These fees should be passed directly to issuers (who run the greatest risk by such non-compliance).

An adjustment that accounts for the failure of merchants to comply with PCI-DSS data security standards would be a fair adjustment of the burden of fraud-prevention. Perhaps even more importantly, it would be a poignant and real spur to merchants to comply with accepted minimum security standards.

VI. Conclusion

In sum, Regions believes that either a fraud-prevention allowance of (a) 2.9¢ per transaction corresponding to a typical issuer's costs or (b) 3.1¢ per transaction based on the costs of the substantial majority of covered issuers would better accomplish the Board's and Congress's fraud-prevention goals and would be a fairer and more reasonable measure for issuers' fraud-prevention costs. Either amount would more accurately reflect the true prevention costs of issuers based on the results of the Board's Survey, as opposed to the costs and economies of scale of the 3 dominant issuers that is reflective of the method currently employed by the Board in its rule-making. Further, Regions believes that the fraud-prevention adjustment should be a percentage of the value of a transaction rather than a set amount for all transactions.

The fraud-prevention adjustment should be required and not a cap because the adjustment is supposed to be an allowance that actually encourages fraud-prevention activities and compliance, not merely an upper limit to a negotiated interchange fee.

In addition, Regions urges that a reasonable allowance should be flexible and provide increases in the fraud-prevention adjustment for (a) issuers' additional investment in fraud prevention technologies and activities, (b) for significant increases in fraudulent activity, and (c) merchants' failure to comply with fraud-prevention standards. Each of these adjustments will further the goals of encouraging effective and innovative fraud-prevention.

As I indicated above, Regions values the opportunity to comment on the proposed regulations and appreciates your consideration of the views expressed in our letter. We would be pleased to discuss our comments further with the Board and its staff.

Sincerely,

Tom Brooks
Executive Vice President
Cards & Payments
Regions Financial Corporation