Wells Fargo & Company
420 Montgomery Street
San Francisco, CA 94104

September 30, 2011

Jennifer J. Johnson, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, N.W.
Washington, DC 20551
regs.comments@federalreserve.gov

Re: Docket No. R-1404; RIN No. 7100-AD 63
Regulation II; Interim Final Rule – Fraud-prevention Adjustment

Dear Ms. Johnson:

This letter is submitted on behalf of Wells Fargo & Company and its affiliates ("Wells Fargo") in response to the Interim Final Rule implementing provisions of Section 1075 of the Dodd Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank Act"), which amends the Electronic Fund Transfer Act ("EFTA"), published in the Federal Register on July 20, 2011 at 76 FR 43478 (the "Interim Final Rule"). Wells Fargo appreciates the opportunity to comment and respectfully requests the members of the Board of Governors of the Federal Reserve System ("Board") to consider adopting the suggestions set forth herein.

The Wells Fargo vision to satisfy all of our customers' financial needs and to help them succeed financially is a driving force in the way we do business. Engaging in responsible lending practices, encouraging consumers to make responsible and successful financial choices and conducting business with honesty and integrity, are already at the heart of our vision. It is our practice to build our business processes and strategies in compliance with all applicable laws and regulations.

While Wells Fargo supports the Board's adoption of a fraud-prevention adjustment to the maximum allowable interchange transaction fee and non-prescriptive standards, this letter provides Wells Fargo's comments to the Interim Final Rule as well as further requests for additional clarification based upon the Interim Final Rule.

Summary of Key Comments:

- **The Fraud-prevention Adjustment is Reasonably Necessary to Make Allowance for Costs Incurred by Issuers in Preventing Fraud and to Ensure Continued Innovation in Fraud-prevention Tools and Activities.** Based on data received by the Board in response to its survey of debit card issuers and networks, the Board estimated that industry-wide fraud losses to all parties to electronic debit transactions were approximately $1.34 billion in 2009. According to issuer survey data, issuers engage in various activities to detect, prevent and mitigate fraudulent electronic debit transactions and incur the costs of such activities. Higher interchange revenues may have helped to offset issuers' fraud losses and fraud-prevention costs and fund innovation in fraud-prevention tools and activities. Given the almost fifty-percent reduction in allowable interchange transaction fees, the fraud-prevention adjustment is imperative to offset issuer costs in preventing fraud and incenting issuers to continue to invest in new fraud-prevention tools and activities.
- **Non-prescriptive Standards Maintain Issuer Flexibility in Responding to New and Evolving Fraud Risks and Help Protect Against Industry-Wide Fraud Impacts in the Event of a Breach.** Wells Fargo strongly supports the Board's adoption of non-prescriptive standards. We agree with the Board that each issuer must determine, based on its own debit card program and fraud experiences, which policies and procedures are reasonably designed to meet the objectives set forth in the standards. It is imperative that issuers have the flexibility to respond quickly and effectively to emerging and evolving fraud risks. To the extent issuers are required to implement the same or similar fraud-prevention technologies, the entire debit card payment system would be at risk in the event of a breach.

Discussion:

I. Section 235.4(a): Fraud-prevention Adjustment

Pursuant to Section 235.4(a) of the Interim Final Rule, if an issuer meets the standards set forth in the Interim Final Rule, it may receive or charge no more than 1 cent per transaction as a fraud-prevention adjustment, in addition to the allowable interchange transaction fee.

A. The Statute Authorizes an Adjustment to the Interchange Transaction Fee for Fraud-prevention Costs

Section 920(a)(5) of the EFTA authorizes the Board to allow for an adjustment to the interchange transaction fee if (i) such adjustment is reasonably necessary to make allowance for costs incurred by the issuer in preventing fraud in relation to electronic debit transactions involving that issuer, and (ii) the issuer complies with fraud-related standards established by the Board. Nothing in the statute requires the Board to limit the adjustment to just 1 cent.

B. The Fraud-prevention Adjustment is Reasonably Necessary to Make Allowance for Costs Incurred by Issuers in Preventing Fraud

Through various meetings and surveys, the Board has gathered information about technological innovation in fraud prevention; fraud risk associated with different types of electronic debit transactions; the nature, type, and occurrence of fraud in electronic debit transactions; the losses absorbed by parties involved in those transactions; and the fraud-prevention and data-security activities and costs, and related research and development costs, incurred by issuers in 2009.[1] Based on the issuer and network survey data, the Board estimated that industry-wide fraud losses to all parties to electronic debit transactions were approximately $1.34 billion in 2009.[2] Issuers identified several categories of activities used to detect, prevent and mitigate fraudulent electronic debit transactions.[3] According to the issuer survey data, the median amount spent by issuers on all reported fraud-prevention activities was approximately 1.8 cents per transaction.[4] The 1.8 cents includes the median amount spent by issuers on transaction monitoring, which was approximately 0.7 cents and which is already included in the permissible interchange transaction fee.[5] Thus, the median amount spent by issuers on fraud-prevention activities, not including transaction monitoring, was approximately 1.1 cents.

While the 1 cent fraud-prevention adjustment helps to alleviate the fifty percent reduction in interchange fees resulting from the final rule on Debit Card Interchange Fees and Routing[6], basing the adjustment on the median amount surveyed issuers reported spending on fraud prevention allows only fifty percent of those issuers to recover the costs they incurred in preventing fraud in relation to electronic debit transactions. According to the Board, "an amount that makes allowance for an issuer's fraud-prevention costs is one that gives consideration to those costs, and allows a *reasonable* recovery of those costs" based on factors specified in Section 920(a)(5)(B)(ii).[7] (Emphasis added). At the 80th percentile, the fraud prevention adjustment would be 2.3

---

[1] 76 FR at 43479

[2] *Id.* at 43480

[3] The categories included transaction monitoring; merchant blocking; card activation and authentication systems; PIN customization; system and application security measures, such as firewalls and virus protection software; and ongoing research and development focused on making an issuer's fraud-prevention practices more effective. 76 FR at 43481

[4] 76 FR at 43481

[5] *Id.*

[6] Debit Card Interchange Fees and Routing. published on July 20, 2011 at 76 Fed. Reg. 43394 ("Final Rule").

[7] 76 FR at 43482

cents per transaction based on the 2009 survey data.[8] There is nothing to indicate that an amount based on the 80th percentile would necessarily be deemed "unreasonable." In fact, the base cost component for the maximum allowable interchange transaction fee was derived, in part, from the per-transaction allowable cost of the surveyed issuers at the 80th percentile.[9]

The fraud-prevention adjustment set forth in the Interim Final Rule represents a base component that relates to the fraud-prevention activities that are currently in place. However, what is not being taken into consideration are the fraud prevention costs associated with certain merchant categories that are inherently risky and size of the transaction. To expand acceptance and increase the utility of debit cards, issuers require adequate compensation for the higher risk inherent in certain transactions and with certain types of merchants. Therefore, Wells Fargo suggests that the Board consider a fraud-prevention adjustment that includes the base component plus an ad valorem component, similar to the calculation for the maximum allowable interchange transaction fee. The ad valorem component of the fraud-prevention adjustment would be a variable multiplier that is a function of the dollar amount of the transaction as well as the type of merchant. While Wells Fargo can appreciate the desire for administrative simplicity, it must be balanced with the desire on the part of all parties to electronic debit transactions to expand the service through increased acceptance and utility.

Preventing issuers from recovering the vast majority of their fraud-prevention costs will likely lead to an increase in declined transactions at the point of sale as issuers are required to become more conservative in authorizations. This will have an adverse impact on consumers and decrease sales for merchants.

C. The One Cent Fraud-prevention Adjustment Does Not Cover a Reasonable Amount of the True Costs Incurred by Issuers Related to Fraud-prevention

In an effort to do what is right for the customer and to ensure merchant and consumer confidence in the payment system, issuers often take additional steps to prevent fraud. For example, issuers review transaction histories and proactively contact customers to confirm transactions. In addition, issuers conduct routine card re-issuance due to merchants' failure to comply with data security requirements. Such proactive measures not only reduce fraud losses, they also reinforce consumer and merchant confidence in the debit card payment system. According to the Board, "the median allowance helps to offset the costs of implementing activities that are effective at reducing fraud losses while placing cost discipline on issuers to ensure that those fraud-prevention activities are also cost effective and recognizing that fraud-prevention costs are incurred by both merchants

[8] Federal Reserve, 2009 Interchange Revenue, Covered Issuer Cost. and Covered Issuer and Merchant Fraud Loss Related to Debit Card Transactions. at 30. The 2.3 cent figure is derived from issuer costs at the 80th percentile as follows: 3.1 cents for fraud prevention costs plus 0.4 cents for data security costs minus 1.2 cents for transaction monitoring costs (although only 0.7 cents was added to the general interchange fee for transaction monitoring costs).

[9] 76 FR at 43422

and issuers."[10] However, it may not be readily apparent whether a fraud-prevention activity is "cost effective" since changes to existing fraud-prevention activities and the implementation of new fraud-prevention activities need to be monitored over time in order to assess their effectiveness and their costs relative to fraud-prevention results. Wells Fargo encourages the Board to continue gathering additional information about the costs for these additional measures, as such measures continually change in response to new and evolving fraud risks.

D. The Fraud-prevention Adjustment is Necessary to Ensure Continued Innovation in Fraud-prevention Tools and Activities

According to Section 920(a)(5)(A)(ii)(II) of the EFTA, the fraud-related standards to be established by the Board must "require issuers to take effective steps to reduce the occurrence of, and costs from, fraud in relation to electronic debit transactions, including through the *development and implementation of cost-effective fraud-prevention technology*." (Emphasis added).

While the maximum interchange transaction fee amount (including the ad valorem component), pursuant to the Final Rule, includes surveyed issuers' median transaction monitoring costs and fraud losses, the survey data makes it very clear that the 0.7 cents included for transaction monitoring costs and the 5 basis points of the transaction included for fraud losses do not represent all fraud-related issuer costs. The Board recognizes that higher interchange revenues, which have now been cut by more than fifty percent, may have allowed issuers to offset both their fraud losses and fraud-prevention costs and fund innovation in fraud-prevention tools and activities.[11] Just as the dynamic nature of the debit card fraud environment requires standards that permit issuers to determine and develop the best methods for detecting, preventing, and mitigating fraud losses for their unique debit card programs, it also requires continued innovation in these methods, and the development of new methods, to respond to continually changing and emerging fraud trends.

Innovation is imperative not only with respect to the development of new fraud-prevention technology and methods, but also with respect to changes and improvements in existing fraud-prevention technology and methods. Innovation helps prevent future fraud losses. Fraud-prevention technology and methods that have been in use for a period of time may become less effective as fraudsters find new ways to circumvent them. While implementing changes to existing technology and methods may often be effective in combating fraud, at least in the short-term, new technology or methods will inevitably need to be developed at considerable expense to issuers. In developing and testing new technology, issuers may ultimately decide not to implement the new technology because it would not be cost-effective even though it may be more effective in combating fraud. For example, smart card systems arguably offer more protection

[10] *Id.* at 43483

[11] *Id.* at 43481

from fraud; however, the increased costs of initial development and implementation may impede their widespread adoption by issuers and merchants. If a fraud-prevention adjustment is not allowed, or is not sufficient to offset many issuer costs, issuers may not invest in new fraud-prevention measures that may initially be less cost-effective but that may be more effective in preventing fraud.

E. Differentiating Between Authentication Methods Would Likely Impede Innovation and Investment

While Wells Fargo had recommended a safe harbor as opposed to a cap on the adjustment, we support the Board's adoption of a fraud-prevention adjustment that is applicable to all transactions, regardless of authentication method. Wells Fargo shares the Board's concern that limiting the adjustment to authentication methods available today may not allow flexibility for issuers to develop other methods of authentication and may reduce incentives for issuers to improve fraud-prevention techniques for systems that experience higher fraud rates.[12] For example, limiting the fraud-prevention adjustment to PIN-based debit transactions may limit investment in new authentication methods, which may actually be more effective than current authentication methods, and may limit fraud-prevention investments for non-PIN transactions.

As the data clearly shows, and as stated in our February 22, 2011 comment letter in response to the Board's proposed rule for the regulation of interchange transaction fees,[13] Wells Fargo strongly believes a fraud-prevention adjustment is imperative as fraud-prevention costs are very real and critical costs incurred by issuers with respect to electronic debit transactions. For the reasons stated above, the fraud-prevention adjustment is necessary to ensure that all issuer fraud-related costs are considered and that innovation in fraud-prevention tools and activities continues, to the benefit of all parties involved in electronic debit transactions.

II. Section 235.4(b): Issuer Standards

A. Non-prescriptive Standards Maintain Issuer Flexibility in Responding to Fraud Risks

The Interim Final Rule requires issuers to develop and implement policies and procedures reasonably designed to identify and prevent fraudulent electronic debit transactions; monitor the incidence of, reimbursements received for, and losses incurred from fraudulent electronic debit transactions; respond appropriately to suspicious electronic debit transactions so as to limit the fraud losses that may occur and prevent the occurrence of future fraudulent electronic debit transactions; and secure debit card and cardholder data. Wells Fargo agrees with the Board that each issuer must determine, based on its own debit card program and fraud experiences, which policies and procedures are reasonably designed to meet the objectives set forth in the standards.

[12] 76 FR at 43483

[13] Debit Card Interchange Fees and Routing, published on December 28, 2010 at 75 Fed. Reg. 81722 ("Proposed Rule").

According to the Interim Final Rule, each issuer's policies and procedures must include fraud-prevention technologies and other methods or practices reasonably designed to detect, prevent, and mitigate fraudulent electronic debit transactions, and should address, among other things, fraud related to unauthorized use (such as stolen cards, merchant employee fraud, and hacking). In addition, implementation of fraud-prevention policies and procedures should include training the issuer's employees and agents, as appropriate.

Wells Fargo strongly supports the Board's adoption of non-prescriptive standards. Such standards allow issuers to respond quickly and effectively to emerging and evolving fraud risks. Wells Fargo agrees with the Board that "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."[14] As noted by the Board, a variety of factors affect fraud trends. For example, data compromises at merchants or third party vendors may not impact all issuers and may have different degrees of impact on affected issuers. Each issuer must have the flexibility to identify the impact, mitigate the effects, and implement changes to prevent additional fraud from occurring. The industry has proven that it is capable of acting quickly and effectively in adopting fraud-prevention standards. As noted in our comment letter to the Proposed Rule, the industry, including networks, issuers, processors and merchants, acted decisively and partnered together in implementing the Card Verification Value program in the early 1990s.

1. Identifying and Preventing Fraudulent Electronic Debit Transactions

According to comment 4(b)(1)(i) to the Interim Final Rule, the issuer's policies and procedures *may include*: (i) an automated mechanism to assess the risk that a particular electronic debit transaction is fraudulent during the authorization process and monitoring sets of transactions initiated with the cardholder's debit card; (ii) practices to support reporting of lost and stolen cards or suspected incidences of fraud by cardholders or other parties to a transaction (e.g., text alerts); and (iii) practices to help determine whether a user is authorized to use the card at the time of a transaction (e.g., use of dynamic data). In addition, the issuer's policies and procedures *should include* an assessment of the effectiveness of the different authentication methods that it enables its cardholders to use, including a review of the rate of fraudulent transactions for each authentication method. The issuer *should also consider* practices to encourage its cardholders to use the more effective authentication method(s) and *should consider* methods for reducing fraud on the less effective authentication methods. Finally, the issuer *should monitor* industry developments and consider adopting, where practical, any new authentication methods that are materially more effective than the issuer's current authentication methods. (Emphasis added).

[14] 76 FR at 43484

With respect to the Board's suggestion that issuers should consider practices to encourage its cardholders to use more effective authentication methods, Wells Fargo agrees with the concept. However, additional investment will be required and factors other than effectiveness must also be considered. While the Board should encourage innovation, it should not pick winners and losers with respect to authentication methods. Each issuer must decide whether or not to encourage the use of a particular authentication method based on a number of factors, including effectiveness, acceptance, utilization, and cost. For example, PIN debit is not available in all card acceptance channels, not accepted by all merchants, and not utilized by all consumers; therefore it is not the best solution in every case.[15] Wells Fargo requests that the Board clarify that effectiveness is only one of the factors that issuers should consider in deciding whether to encourage the use of a particular authentication method and that other factors and circumstances impact available authentication methods.

With respect to the Board's suggestion that issuers should monitor industry developments and consider adopting, where practical, any new authentication methods that are materially more effective than the issuer's current authentication methods, Wells Fargo is concerned that the Interim Final Rule does not define "materially more effective." Wells Fargo requests that the Board clarify that each issuer must determine, for itself, whether a given authentication method utilized in the industry is materially more effective than its current authentication methods. Wells Fargo also requests that the Board clarify that issuers are not required to adopt any specific authentication methods, whether or not they are arguably "materially more effective." As stated above, Wells Fargo agrees with the Board that each issuer must determine which methods to detect, prevent, and mitigate fraud losses are best, based on the size and scope of its debit card business, which is consistent with the Board's suggestion that new authentication methods be adopted *where practical*. (Emphasis added). To require the adoption of specific industry authentication methods would deter from the Board's adoption of non-prescriptive standards and subject the debit card industry to greater fraud risk in the event such authentication methods are compromised by fraudsters.

The Board requested comment on whether the policies and procedures should require an issuer to assess whether its customer rewards or similar programs provide inappropriate incentives to use an authentication method that is demonstrably less effective in preventing fraud. Wells Fargo does not believe such a requirement should be implemented. Issuers already consider a variety of factors in assessing the appropriateness and value, to all parties to electronic debit transactions, of incenting the use of particular authentication methods and entering into partnerships to encourage the use of debit cards. Fraud risk is only one of many factors that issuers consider in deciding whether to offer specific

[15] In the preamble to the Proposed Rule, the Board noted its understanding that of the 8 million merchant locations in the United States that accept debit cards, only 2 million have the capability to accept PIN debit transactions. *See* 75 FR at 81749

incentive programs. For example, issuers may enter into partnerships with merchants to encourage merchant sales and the use of the issuer's debit cards. Some merchants may accept both PIN and signature transactions and some may accept only signature transactions. It is the issuer's decision, based on all factors relevant to its debit card program and business, whether or not to enter into, or maintain, such partnerships. In addition, the Final Rule sets a maximum permissible interchange transaction fee that an issuer may receive for electronic debit transactions, irrespective of authentication method, essentially eliminating that financial incentive to encourage the use of a particular authentication method.

2. Responding Appropriately to Suspicious Electronic Debit Transactions

Pursuant to the Interim Final Rule, the issuer must have policies and procedures in place designed to implement an appropriate response once an issuer has identified suspicious transactions or transactions likely to be fraudulent. Wells Fargo agrees with the Board that an appropriate response will likely differ depending on the circumstances and the risk of future fraudulent electronic debit transactions. However, Wells Fargo requests that the Board clarify that the assessment of the risk will vary based on each issuer's debit card program and specific fraud experiences and data analysis. For example, an issuer may decide not to reissue cards in certain cases of suspected fraud and may instead choose to monitor the account for some period of time. Arguably, reissuing the card would ensure that the old card could not be used to conduct future fraudulent transactions. However, if the issuer's experience and data indicated that future fraudulent transactions were unlikely with the old card, in issuing new cards the issuer would incur potentially unnecessary costs of reissuance and consumers would be needlessly inconvenienced.

3. Securing Debit Card and Cardholder Data

According to comment 4(b)(1)(iv)-1 to the Interim Final Rule, the issuer's policies and procedures must be designed to secure debit card and cardholder data transmitted by the issuer (or its service provider) during transaction processing, stored by the issuer (or its service provider), and carried on media (e.g., laptops) by employees or agents of the issuer. This standard may be incorporated into the issuer's information security program (as required by the Gramm-Leach-Bliley Act). However, Wells Fargo notes that the Supplementary Information to the Interim Final Rule indicated that the issuer's policies and procedures must be designed to secure debit card and cardholder data transmitted "to or from" an issuer or its service provider during transaction processing.[16] Wells Fargo requests clarification that the requirement to secure debit card and cardholder data applies only to debit card and cardholder data transmitted "by" the issuer or its service provider. Issuers cannot control the transmission of data from third parties with whom the issuer has not specifically contracted for such submissions.

[16] 76 FR at 43485

B. Non-prescriptive Standards Help Protect Against Industry-wide Fraud Impacts in the Event of a Breach

Wells Fargo agrees with the Board that "specifying, and limiting the set of, technologies for which issuers recover their costs may weaken the long-term effectiveness of these technologies."[17] As we stated in our February 22, 2011 comment letter in response to the Proposed Rule, publishing technology-specific standards would provide fraudsters with valuable information, which would allow them to adapt to and overcome the standards and increase the rate of fraud. Further, to the extent the entire industry is required to utilize the same or similar fraud prevention technologies, the entire debit card system would be at risk in the event of a breach. Such an industry-wide impact would not only result in increased fraud losses, but would also undermine the confidence of consumers, merchants, and issuers in the debit card payment system.

C. The Board's Proposed Definition of "Fraud"

Section 903(11) of the EFTA defines "unauthorized electronic fund transfer" as "an electronic fund transfer from a consumer's account initiated by a person other than the consumer without actual authority to initiate such transfer and from which the consumer receives no benefit, but does not include any electronic fund transfer (A) initiated by a person other than the consumer who was furnished with the card, code or other means of access to such consumer's account by such consumer, unless the consumer has notified the financial institution involved that transfers by such other person are no longer authorized, (B) initiated with fraudulent intent by the consumer or any person acting in concert with the consumer, or (C) which constitutes an error committed by a financial institution." In the preamble to the Proposed Rule, the Board suggested that fraud in the debit card context should be defined as "the use of a debit card (or information associated with a debit card) by a person, other than the cardholder, to obtain goods, services, or cash without authority for such use." Wells Fargo agrees with the Board that whether a transaction is in fact fraudulent will depend on the facts and circumstances of the transaction. However, Wells Fargo urges the Board to adopt a broader definition of fraud based on the EFTA's definition of "unauthorized electronic fund transfer." For example, fraud in the debit card context could be defined as "the use of a debit card (or information associated with a debit card): (i) by a person, other than the cardholder, to obtain goods, services, or cash without authority for such use and from which the cardholder receives no benefit, or (ii) by a cardholder, or any person acting in concert with a cardholder, with fraudulent intent." Wells Fargo also agrees that the policies and procedures need not necessarily address types of fraud, such as unauthorized transactions with a fraudulent merchant, that issuers generally have very limited ability to control. However, issuers should have the ability to choose to include policies and procedures to minimize such fraudulent transactions.

[17] *Id.* at 43484

D. Annual Review of Policies and Procedures

The Interim Final Rule requires each issuer to review its fraud-prevention policies and procedures at least annually, and update them as necessary to address changes in the prevalence and nature of fraudulent electronic debit transactions and available methods of detecting, preventing, and mitigating fraud. The issuer may need to review and update its policies and procedures more frequently. For example, additional review and updates may be necessary if there is a significant change in fraud types, fraud patterns, or fraud-prevention methodologies or technologies. Wells Fargo agrees that each issuer should review its policies and procedures on an annual basis. Such review should be concurrent with the issuer's certification to its payment card networks that the issuer's policies and procedures meet the fraud-prevention standards. However, rather than requiring additional review and updates based on a "significant change," which is not defined in the Interim Final Rule, Wells Fargo requests that the Board clarify that the issuer should determine whether any change in fraud types, fraud patterns, or fraud-prevention technologies or methodologies has an impact on its specific policies and procedures that would require additional review and updates.

E. Certification

Pursuant to the Interim Final Rule, payment card networks that choose to allow issuers to receive or charge a fraud-prevention adjustment must develop their own processes for identifying issuers eligible for the adjustment. In order to receive or charge a fraud-prevention adjustment, the issuer must certify its compliance with the standards, and eligibility, to its payment card networks on an annual basis. Wells Fargo believes that each payment card network should establish its own certification process for the fraud-prevention adjustment. This will allow each network to establish processes that are consistent with its other processes for tracking exempt versus non-exempt issuers and issuer certifications of products that are eligible for an exemption from the interchange fee provisions.

III. Effective Date

The Interim Final Rule is effective October 1, 2011. In order to receive the fraud-prevention adjustment, issuers must comply with the Board's fraud-prevention standards by that date. Wells Fargo agrees that the Interim Final Rule should be effective concurrently with the Final Rule.

Conclusion

Wells Fargo strives to provide our customers with flexible, wide-ranging and competitive financial products, superior service and education while fully complying with all applicable laws and regulations. We strongly support the Board's adoption of a fraud-prevention adjustment and non-prescriptive standards. However, we respectfully urge the Board to consider all of the comments and suggestions herein.

If you have any questions or would like to discuss any of the issues herein, please do not hesitate to contact me at (612) 667-4025 or dawn.m.mandt@wellsfargo.com.

Sincerely,

/s/ DAWN M. VAIL

Dawn M. Vail
Senior Counsel