FEDERAL RESERVE SYSTEM

12 CFR Part 235

Regulation II; Docket No. R-1404

RIN No. 7100-AD 63

Debit Card Interchange Fees and Routing

AGENCY: Board of Governors of the Federal Reserve System

ACTION: Final rule

SUMMARY: The Board has amended the provisions in Regulation II (Debit Card Interchange Fees and Routing) that govern adjustments to debit card interchange transaction fees to make an allowance for fraud-prevention costs incurred by issuers. The amendments permit an issuer to receive or charge an amount of no more than 1 cent per transaction (the same amount currently permitted) in addition to its interchange transaction fee if the issuer develops and implements policies and procedures that are reasonably designed to take effective steps to reduce the occurrence of, and costs to all parties from, fraudulent electronic debit transactions. The amendments set forth fraud-prevention aspects that an issuer's policies and procedures must address and require an issuer to review its policies and procedures at least annually, and update them as necessary in light of their effectiveness, cost-effectiveness, and changes in the types of fraud, methods used to commit fraud, and available fraud-prevention methods. An issuer must notify its payment card networks annually that it complies with the Board's fraud-prevention standards. Finally, the amendments provide that an issuer that is substantially noncompliant with the Board's fraud-prevention standards is ineligible to receive or charge a fraud-prevention adjustment and set forth a timeframe within which an issuer must stop receiving or charging a fraud-prevention adjustment.

DATES: This rule is effective October 1, 2012.

FOR FURTHER INFORMATION CONTACT: Dena L. Milligan, Attorney (202/452-3900), Legal Division, or David Mills, Manager and Economist (202/530-6265), Division of Reserve Bank Operations and Payment Systems; for users of Telecommunications Device for the Deaf (TDD) only, contact (202/263-4869); Board of Governors of the Federal Reserve System, 20th and C Streets, N.W., Washington, DC 20551.

SUPPLEMENTARY INFORMATION

I. Section 920 of the Electronic Fund Transfer Act

The Dodd-Frank Wall Street Reform and Consumer Protection Act (the "Dodd-Frank Act") (Pub. L. No. 111-203, 124 Stat. 1376 (2010)), was enacted on July 21, 2010. Section 1075 of the Dodd-Frank Act amends the Electronic Fund Transfer Act ("EFTA") (15 U.S.C. § 1693 et

seq.) by adding a new section 920 regarding debit card interchange transaction fees and rules for payment card transactions.

Section 920 of the EFTA provides that, effective July 21, 2011, the amount of any interchange transaction fee that an issuer receives or charges with respect to an electronic debit transaction must be reasonable and proportional to the cost incurred by the issuer with respect to the transaction.[1] This section requires the Board to establish standards for assessing whether an interchange transaction fee is reasonable and proportional to the cost incurred by the issuer with respect to the transaction and requires the Board to establish rules prohibiting network exclusivity on debit cards and issuer and network inhibitions on merchant transaction routing choice. The Board's final rule (Regulation II, Debit Card Interchange Fees and Routing) implementing standards for assessing whether interchange transaction fees meet the requirements of Section 920(a) and establishing rules regarding network exclusivity and routing choice required by Section 920(b) became effective October 1, 2011, although issuers had until April 1, 2012, or later to comply with the network exclusivity provisions.[2]

Under EFTA Section 920(a)(5), the Board may allow for an adjustment to the amount of an interchange transaction fee received or charged by an issuer if (1) such adjustment is reasonably necessary to make allowance for costs incurred by the issuer in preventing fraud in relation to electronic debit card transactions involving that issuer, and (2) the issuer complies with fraud-prevention standards established by the Board. Those standards must be designed to ensure that any adjustment is limited to the reasonably necessary fraud-prevention allowance described in clause (1) above; takes into account any fraud-related reimbursements (including amounts from chargebacks) received from consumers, merchants, or payment card networks in relation to electronic debit transactions involving the issuer; and requires 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.

In issuing the standards and prescribing regulations for the adjustment, EFTA Section 920(a)(5) requires the Board to consider (1) the nature, type, and occurrence of fraud in electronic debit transactions; (2) the extent to which the occurrence of fraud depends on whether the authentication in an electronic debit transaction is based on a signature, personal identification number (PIN), or other means; (3) the available and economical means by which fraud on electronic debit transactions may be reduced; (4) the fraud-prevention and data-security costs expended by each party involved in the electronic debit transactions (including consumers, persons who accept debit cards as a form of payment, financial institutions, retailers, and payment card networks); (5) the costs of fraudulent transactions absorbed by each party involved in such transactions (including consumers, persons who accept debit cards as a form of payment, financial institutions, retailers, and payment card networks); (6) the extent to which interchange

[1] An "electronic debit transaction" means the use of a debit card (including a general-use prepaid card) as a form of payment. EFTA Section 920(c)(5); 12 CFR § 235.2(h). For purposes of Regulation II, the term does not include transactions initiated at automated teller machines (ATM).

[2] 76 FR 43394, 43394 (Jul. 20, 2011). Regulation II is set forth in 12 CFR part 235. Regulation II defines an interchange transaction fee (or "interchange fee") to mean any fee established, charged, or received by a payment card network and paid by a merchant or acquirer for the purpose of compensating an issuer for its involvement in an electronic debit transaction. 12 CFR § 235.2(j).

transaction fees have in the past reduced or increased incentives for parties involved in electronic debit transactions to reduce fraud on such transactions; and (7) such other factors as the Board considers appropriate.

II. Proposed Rule, Interim Final Rule, and Comments

A. Proposed Rule

In December 2010, the Board requested comment on two approaches to a framework for the fraud-prevention adjustment to the interchange transaction fee standards: a technology-specific approach and a non-prescriptive approach. The technology-specific approach would allow an issuer to recover some or all of its costs incurred for implementing major innovations that would likely result in substantial reductions in total, industry-wide fraud losses. Under this approach, the Board would identify paradigm-shifting technologies that would reduce debit card fraud in a cost-effective manner. The alternative approach would establish more general standards that an issuer must meet to be eligible to receive an adjustment for fraud-prevention costs.[3]

In general, commenters did not agree about which approach to pursue, but commenters generally opposed the Board's mandating use of specific technologies. Most merchants generally favored a paradigm-shifting approach where issuers would be eligible for a fraud-prevention adjustment only for implementing technologies that reduced fraudulent transactions to a level materially below the level for PIN transactions. By contrast, issuers of all sizes and payment card networks preferred the non-prescriptive approach that would provide issuers with flexibility to tailor their fraud-prevention activities to address most effectively the risks they face and changing fraud patterns. Issuer commenters also opposed a fraud-prevention adjustment only for particular authentication methods, noting that an adjustment favoring a particular authentication method may not provide sufficient incentives to invest in other potentially more effective authentication methods.[4] The Board considered these comments in the development of an interim final rule.

B. Interim Final Rule

In June 2011, the Board adopted a non-prescriptive approach to the fraud-prevention standards, set forth in 12 CFR § 235.4, as an interim final rule, issued in connection with its final rule implementing other provisions of EFTA Section 920.[5] The interim final rule allows an issuer to receive or charge an additional amount of no more than 1 cent per transaction to the interchange fee permitted under § 235.3 if the issuer satisfies the Board's fraud-prevention standards. Those standards require an issuer to develop and implement policies and procedures reasonably designed to (i) identify and prevent fraudulent electronic debit transactions; (ii) monitor the incidence of, reimbursements received for, and losses incurred from fraudulent electronic debit transactions; (iii) respond appropriately to suspicious electronic debit

[3] 75 FR 81722, 81740-43 (Dec. 28, 2010).
[4] The comments received by the Board in response to the proposal are described in more detail in the *Federal Register* notice announcing the interim final rule. *See* 76 FR 43478, 43480-86 (Jul. 20, 2011).
[5] The final rule implementing other provisions in Regulation II is published in 76 FR 43394 (Jul. 20, 2011).

transactions so as to limit the fraud losses that may occur and prevent the occurrence of future fraudulent electronic debit transactions; and (iv) secure debit card and cardholder data. In addition, an issuer must 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 the available methods of detecting, preventing, and mitigating fraud. The interim final rule provides that if an issuer meets these standards and wishes to receive the adjustment, it must annually certify its compliance with the Board's fraud-prevention standards to the payment card networks in which the issuer participates. The Board requested comment on all aspects of the interim final rule.

C. Summary of Comments on Interim Final Rule

The Board received 42 comments on the interim final rule from debit card issuers, depository institution trade associations, payment card networks, merchants, merchant trade associations, a card-payment processor, technology companies, a member of Congress, individuals, and public interest groups.

1. Overview of Comments Received

The comments received generally focused on the following aspects of the interim final rule: (1) the amount of the adjustment; (2) the non-prescriptive standards in the interim final rule; and (3) the issuer-certification process. These comments are summarized below and are described in more detail in the **Section-By-Section Analysis**.

Fraud-prevention adjustment amount. Most issuers and their trade associations, payment card networks, a public interest group, and a technology company supported permitting a fraud-prevention adjustment to the amount of an interchange transaction fee an issuer may receive or charge but believed the fraud-prevention adjustment amount in the interim final rule to be too low. Commenters that supported a higher adjustment amount did so for several reasons, including encouraging innovation and investment in fraud-prevention activities; maintaining consumer and merchant confidence in the security of electronic debit transactions; and reducing potential adverse effects on exempt issuers that have higher per-transaction fraud-prevention costs than nonexempt issuers. These commenters suggested that the Board could increase the adjustment amount by expanding the costs used in determining the adjustment amount; setting the adjustment amount to the fraud-prevention amount at the cost of the issuer at the 80th percentile (as with the interchange fee standard in § 235.3) rather than at the median issuer's cost; including an additional *ad valorem* component to the adjustment; and not capping the adjustment amount. Commenters suggested including costs such as fraud-prevention research and development costs, data-security costs, fraud-related customer inquiry costs, and exempt issuer costs.

By contrast, merchants and their trade associations asserted that the fraud-prevention adjustment amount in the interim final rule is too high. In general, these commenters argued that the fraud-prevention amount in the interim final rule does not take into consideration the fraud-prevention costs of merchants and other parties to electronic debit transactions, for example, by deducting merchants' costs from issuers' costs. Several of these commenters recommended that, in setting the adjustment amount, the Board include only activities that are demonstrably

effective and cost-effective, and one commenter recommended that the Board exclude costs of activities to *detect* and *mitigate* fraudulent electronic debit transactions.

Approach to fraud-prevention standards. Debit card issuers, their trade associations, and payment card networks overwhelmingly supported the non-prescriptive framework for the fraud-prevention standards largely as set forth in the interim final rule for several reasons.[6] These reasons included providing better incentives to invest in fraud prevention, retaining flexibility for each issuer to respond effectively to the dynamic fraud environment, diversifying fraud-prevention technologies employed throughout the industry, and limiting public information about issuers' fraud-prevention activities, which, commenters argued, could benefit fraudsters. In addition, several commenters opposed a technology-specific adjustment, arguing that the Board does not have the expertise to identify the most effective and commercially feasible fraud-prevention technologies and that such an approach could result in underinvestment in new, and potentially more effective, fraud-prevention technologies that are not identified in the standards.

By contrast, most merchants and merchant trade associations, a public interest group, and a member of Congress opposed the fraud-prevention standards as set forth in the interim final rule because the standards do not include specific metrics to measure the effectiveness and cost-effectiveness of an issuer's fraud-prevention activities. Several of these commenters argued that fraud-prevention standards that lack such a metric are inconsistent with EFTA 920(a)(5). A number of these commenters supported a proposal made by a coalition of merchants. This proposal suggested metrics for measuring the effectiveness and cost-effectiveness of fraud-prevention activities that would assess whether the fraud-prevention technology results in a fraud rate materially lower than that associated with PIN transactions and whether the cost of implementing a technology is less than the amount of fraud losses eliminated by its use.

In contrast to the other commenters, several technology companies supported the specification of particular fraud-prevention technologies in the Board's standards.

Issuer certification. The Board received several comments about the certification process in § 235.4(c). Many commenters opposed the "certification" requirement in the interim final rule because they believed it improperly delegates assessment of an issuer's compliance from an issuer's primary supervisor to an issuer or payment card network. Other commenters supported the certification requirement as described in the interim final rule or requested clarification about the role of payment card networks in the certification process. Commenters also disagreed as to whether the Board should specify a uniform certification process and reporting period. In addition, one payment card network supported a so-called "cure period" for issuers to come into compliance with the Board's fraud-prevention standards after a deficiency finding and a 30-day time period for networks to change the status of an issuer once a network is notified of an issuer's noncompliance with the Board's standards.

2. Consultation with Other Agencies

EFTA Section 920(a)(4)(C) directs the Board to consult, as appropriate, with the Comptroller of the Currency, the Board of Directors of the Federal Deposit Insurance

[6] The Board received some comments suggesting more targeted clarifications to the rule text and commentary. These comments are discussed below in connection with the relevant rule or commentary section.

Corporation, the National Credit Union Administration Board, the Administrator of the Small Business Administration, and the Director of the Bureau of Consumer Financial Protection in the development of the interchange fee standards. Board staff consulted with staff from these agencies in development of a final rule on standards for receiving or charging a fraud-prevention adjustment.

III. Statutory Considerations

EFTA Section 920(a)(5) requires the Board to consider several different factors in prescribing regulations related to the fraud-prevention adjustment. This section discusses each of those factors.

Nature, type, and occurrence of fraud. The Board's survey of debit card issuers and payment card networks provided information about the nature, type, and occurrence of fraud in electronic debit transactions.[7] From the card issuer and network surveys of 2009 data, the Board estimates that industry-wide fraud losses to all parties to debit card transactions were approximately $1.34 billion in 2009.[8] Based on data provided by covered issuers, about 0.04 percent of purchase transactions were fraudulent, with an average loss per purchase transaction of about 4 cents, or about 9 basis points of transaction value.[9]

The most commonly-reported and highest-value fraud types were counterfeit card fraud; mail, telephone, and Internet order (or "card-not-present") fraud; and lost and stolen card fraud.[10] Counterfeit card fraud represented 0.01 percent of all purchase transactions, with an average loss of 2 cents per transaction and 4 basis points of transaction value. Mail, telephone, and Internet order fraud also represented 0.01 percent of all purchase transactions with an average loss of 1 cent per transaction and 2 basis points of transaction value. Lost and stolen card fraud represented less than 0.01 percent of all purchase transactions with an average loss of 1 cent per transaction and 1 basis point of transaction value.

Extent to which the occurrence of fraud depends on authentication mechanism. The issuer survey data for 2009 also provided information about the extent to which the occurrence

[7] The Board's "2009 Interchange Revenue, Covered Issuer Cost, and Covered Issuer and Merchant Fraud Loss Related to Debit Card Transactions" is available at *http://www.federalreserve.gov/paymentsystems/regii-data-collections.htm.*

[8] Unless otherwise noted, debit card transactions include transactions initiated using general-use prepaid cards. Industry-wide fraud losses were extrapolated from data reported in the issuer and network surveys conducted by the Board. Of the 89 issuers that responded to the issuer survey, 52 issuers provided data on fraud losses related to their debit card transactions. These issuers reported $726 million in fraud losses to all parties of card transactions and represented 54 percent of the total transactions reported by networks.

[9] Covered issuers are those issuers that, together with affiliates, have assets of $10 billion or more. *See* 12 CFR § 235.5(a). The percent of purchase transactions that are fraudulent is the number of fraudulent transactions divided by the number of purchase transactions. The average loss per purchase transaction is the dollar amount of fraud losses divided by the number of purchase transactions. The average loss per purchase transaction in basis points is the dollar amount of fraud losses divided by the dollar amount of purchase transactions.

[10] Some issuers reported ATM fraud, which was excluded from fraud loss totals because an ATM transaction does not come under the definition of an "electronic debit transaction." *See* 12 CFR § 235.2(h).

of fraud depends on whether the transaction was processed by a signature or a PIN network.[11] Of the approximately $1.34 billion estimated industry-wide fraud losses, about $1.11 billion of these losses arose from signature debit card transactions and about $181 million arose from PIN debit card transactions.[12] The higher losses for signature debit card transactions are attributable to both a higher rate of fraud and higher transaction volume for signature debit card transactions.[13] The data showed that about 0.06 percent of signature debit and 0.01 percent of PIN debit purchase transactions were reported as fraudulent. For signature debit, the average loss was 5 cents per transaction, and represented about 13 basis points of transaction value. For PIN debit, the average loss was 1 cent per transaction, and was about 3 basis points of transaction value. Thus, on a per-dollar basis, signature debit fraud losses were approximately 4 times PIN debit fraud losses.[14]

The different fraud loss rates for signature and PIN transactions reflect, in part, differences in the ease of committing fraud associated with the two card- and cardholder-authentication methods. A signature debit card transaction requires information that is typically contained on the card itself in order for card and cardholder authentication to take place. Therefore, a thief need only steal the card or information on the card in order to commit fraud.[15] By contrast, card- and cardholder-authentication of a PIN debit card transaction requires not only the card or information contained on the card, but also something only the cardholder should know, namely, the PIN. In the case of PIN transactions, a thief generally needs both the card, or information on the card, and the cardholder's PIN to commit fraud. Virtually all PIN debit transactions currently occur in a card-present environment, and virtually all transactions in card-not-present environments (i.e., Internet) are routed over signature debit networks. For Internet transactions, the cardholder typically does not authenticate the transaction with a signature, although an issuer or merchant may have other means of authenticating the cardholder or card, such as the use of a Card Verification Value (CVV) number or the input of cardholder information at the time of purchase.

Card issuers responding to the Board's survey reported that card-present fraud losses for signature debit transactions were over 3 times greater than the fraud loss value, in basis points, associated with PIN debit card-present transactions. Issuers also reported that fraud losses across all parties on transactions over signature debit networks were higher for card-not-present

[11] Transactions processed over a signature debit network are referred to sometimes as "signature debit card transactions" or "signature debit transactions." Transactions processed over a PIN debit network are referred to sometimes as "PIN debit card transactions" or "PIN debit transactions."

[12] The sum of card program fraud losses does not equal the industry-wide fraud losses due to different sample sizes and rounding.

[13] In 2009, signature transactions accounted for 60 percent of electronic debit transaction volume and 59 percent of transaction value. PIN transactions accounted for 37 percent of electronic debit transaction volume and 39 percent of transaction value. The remainder of the transaction volume and value was attributable to prepaid card transactions, which could be either signature or PIN transactions. *See* 2009 Interchange Revenue, Covered Issuer Cost, and Covered Issuer and Merchant Fraud Loss Related to Debit Card transactions.

[14] The survey data did not break out prepaid card PIN transactions from prepaid card signature transactions. For all prepaid debit transactions, about 0.03 percent of purchase transactions were fraudulent; the average loss was 1 cent per transaction, and 4 basis points of transaction value.

[15] Among other things, information on the card includes the card number, the cardholder's name, and the cardholder's signature.

transactions than for card-present transactions.[16] On a transactions-weighted average basis, card-not-present fraud losses represented 17 basis points of the value of card-not-present signature debit transactions. Card-present fraud losses represented 11 basis points of the value of card-present signature debit transactions.

Available and economical means by which fraud may be reduced. The Board requested information about issuers' fraud-prevention activities and costs in its survey. Issuers identified several categories of activities used to detect, prevent, and mitigate fraudulent electronic debit transactions, including 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.

Based on reported information, the median issuer spent 1.8 cents per transaction on all fraud-prevention activities. The most commonly reported activity in the fraud-prevention section of the survey was transaction monitoring, which generally includes activities related to the authorization of a particular electronic debit transaction, such as the use of neural networks and automated fraud risk scoring systems that may lead to the denial of a suspicious transaction. At the median, issuers reported spending approximately 0.7 cents per transaction on transaction monitoring activity.[17] The costs associated with research and development, card-activation systems, PIN customization, merchant blocking, and card-authentication systems were all small when measured on a per-transaction basis, typically less than one-tenth of a cent each. For all data-security costs reported by issuers in the issuer card survey, the median was 0.1 cents.

Fraud-prevention costs expended by parties involved in electronic debit transactions. As discussed above, issuers incur costs for a variety of fraud-prevention activities. In addition, other parties involved in debit card transactions incur fraud-prevention costs. For example, some consumers routinely monitor their accounts for unauthorized debit card purchases, which could be measured as an opportunity cost of the consumers' time; however, the opportunity cost of consumers' time to monitor their account is difficult to put into monetary terms. Merchants and acquirers incur costs for fraud-prevention tools such as terminals that enable merchants to use various card- and cardholder-authentication mechanisms, address verification, geolocation services, and data-encryption technologies. In addition to services they may purchase from others, merchants may develop their own fraud-prevention tools. For example, many large Internet merchants implement extra security measures to verify the legitimacy of a purchase. Typically these checks occur between the time a transaction is authorized by the issuer and the product is shipped to the purchaser. In their comments on the proposed rule, several online merchants noted that they have developed sophisticated fraud-risk management systems that include both manual review and automated processes, which have reduced fraud rates to levels at or below card-present rates at other merchants. In addition to these investments, merchants also take steps to secure data and comply with Payment Card Industry Data Security Standards (PCI-DSS).[18] In their comments on the proposed rule and interim final rule, several merchants noted

[16] In 2009, almost all card-not-present transactions were processed over signature networks.

[17] Transaction monitoring costs were included in the costs used as the basis for the interchange fee standard rather than the fraud-prevention adjustment. *See* 76 FR 43478, 43482-83 (Jul. 20, 2011).

[18] The Payment Card Industry (PCI) Security Standards Council was founded in 2006 by five card networks—Visa, Inc., MasterCard Worldwide, Discover Financial Services, American Express, and JCB International. These card

that merchants incur substantial costs for PCI-DSS compliance as well as other fraud-prevention activities.

Costs of fraudulent transactions absorbed by different parties involved in fraudulent transactions. Various laws and regulations allocate the costs of fraudulent electronic debit transactions among different parties to the transactions. For example, the Consumer Financial Protection Bureau's Regulation E limits a consumer's liability for unauthorized electronic fund transfers to $50 in certain circumstances.[19] In addition, payment card network rules implement a chargeback process to allocate loss between issuers and acquirers, either of which may, if permitted by network rules, pass on some or all of the loss to the cardholder or merchant. Typically, the allocation of fraud losses under network rules varies by the type of transaction, cardholder authentication method, and procedures followed at the point of sale, among other factors.

Using the issuer survey data for 2009, the Board estimated the cost of fraudulent transactions absorbed by different parties to debit card transactions. Based on the issuer survey responses, almost all of the reported fraud losses associated with debit card transactions fall on the issuers and merchants. In particular, across all types of transactions, 62 percent of reported fraud losses were borne by issuers and 38 percent were borne by merchants. The fraud loss borne by cardholders is low in dollar terms, but may also include costs associated with the time spent rectifying fraudulent transactions. Most issuers reported that they impose zero or very limited liability on cardholders, even where they would be permitted to impose some liability under the EFTA and Regulation E. Payment card networks and merchant acquirers also reported that they bore very limited fraud losses, indicating that merchant acquirers pass through fraud losses to merchants.

The distribution of fraud losses between issuers and merchants varies based on the authentication method used in a debit card transaction. Issuers and payment card networks reported that nearly all the fraud losses associated with PIN debit card transactions (96 percent) were borne by issuers. By contrast, reported fraud losses were distributed much more evenly between issuers and merchants for signature debit card transactions. Specifically, issuers and merchants bore 59 percent and 41 percent of signature debit fraud losses, respectively.[20]

The distribution of fraud losses also varies based on whether or not the card was present at the point of sale. According to the survey data, merchants assume approximately 74 percent of signature debit card fraud for card-not-present transactions, compared to 23 percent for card-present signature debit card fraud.

Extent to which interchange transaction fees have in the past affected fraud-prevention incentives. Issuers have a strong incentive to protect cardholders and reduce fraud independent of interchange fees received. Competition among issuers for cardholders suggests that protecting

---

brands share equally in the governance of the organization, which is responsible for development and management of PCI Data Security Standards (PCI-DSS). PCI-DSS is a set of security standards that all payment system participants, including merchants and processors, are required to meet in order to participate in payment card systems.

[19] *See* 12 CFR § 1005.6.

[20] For prepaid card transactions, issuers bore two-thirds and merchants bore one-third of fraud losses.

their cardholders from fraud is good business practice for issuers. Higher interchange revenues may have allowed issuers to offset both their fraud losses and fraud-prevention costs and fund innovation on fraud-prevention tools and activities. Merchant commenters stated that, historically, the higher interchange revenue for signature debit relative to PIN debit has encouraged issuers to promote the use of signature debit over PIN debit, even though signature debit has substantially higher rates of fraud.

IV. Summary of Final Rule

The Board has considered all comments received and has adopted a final rule for the fraud-prevention adjustment to the amount of an interchange transaction fee that an issuer may receive or charge. The final rule permits an issuer that satisfies the Board's fraud-prevention standards to receive or charge an amount of no more than 1 cent per transaction in addition to any interchange transaction fee it receives or charges in accordance with § 235.3, the same amount as permitted in the interim final rule. The final rule emphasizes the statutory requirements by establishing fraud-prevention standards that require an issuer to develop and implement policies and procedures reasonably designed to take effective steps to reduce the occurrence of, and costs to all parties from, fraudulent electronic debit transactions, including through the development and implementation of cost-effective fraud-prevention technology. An issuer's policies and procedures must address (1) methods to identify and prevent fraudulent electronic debit transactions; (2) monitoring of the volume and value of its fraudulent electronic debit transactions; (3) appropriate responses to suspicious electronic debit transactions in a manner designed to limit the costs to all parties from and prevent the occurrence of future fraudulent electronic debit transactions; (4) methods to secure debit card and cardholder data; and (5) such other factors as the issuer considers appropriate.

The final rule requires an issuer to review its fraud-prevention policies and procedures, and their implementation, at least annually, and update them as necessary in light of (i) their effectiveness in reducing the occurrence of, and cost to all parties from, fraudulent electronic debit transactions involving the issuer; (ii) their cost-effectiveness; and (iii) changes in the types of fraud, methods used to commit fraud, and available methods for detecting and preventing fraudulent electronic debit transactions that the issuer identifies from (A) its own experience or information; (B) information provided to the issuer by its payment card networks, law enforcement agencies, and fraud-monitoring groups in which the issuer participates; and (C) applicable supervisory guidance.

To be eligible to receive or charge a fraud-prevention adjustment, an issuer must annually notify its payment card networks that it complies with the Board's fraud-prevention standards. Finally, if an issuer is substantially noncompliant with the Board's fraud-prevention standards, as determined by the issuer or the agency with responsibility for enforcing the issuer's compliance with Regulation II, the issuer must notify its payment card networks that it is no longer eligible to receive or charge a fraud-prevention adjustment no later than 10 days after the date of the issuer's determination or notification from the agency and must stop receiving or charging the fraud-prevention adjustment no later than 30 days after notifying its networks.

The Board made various changes throughout § 235.4, and accompanying commentary, in response to comments and additional information available to it. The final rule is explained more fully below.

Section-By-Section Analysis

I. Section 235.4(a) Adjustment Amount

A. Summary of Interim Final Rule

Section 235.4(a) of interim final rule permits an issuer to increase the amount of the interchange fee it may receive or charge under § 235.3 by no more than 1 cent if the issuer complies with the Board's fraud-prevention standards in § 235.4(b) of the interim final rule. The adjustment amount is the same irrespective of authentication method, transaction type, or issuer.

The Board surveyed issuers regarding their total cost incurred in 2009 for fraud-prevention and data-security activities, as well as for research and development activities related to an issuer's fraud-prevention program. The Board also asked issuers to report the costs associated with the following: card-activation systems, PIN customization, merchant blocking, transaction monitoring, specialized authorization services, cardholder-authentication systems, card-authentication systems, data-access controls, and data encryption. The Board also invited issuers to report other fraud-prevention and data-security activities, and the costs incurred from those activities.

The interim final rule included costs related to activities used by issuers to "detect, prevent, and mitigate" fraudulent electronic debit transactions, as reported by issuers in the Board survey.[21] For example, the interim final rule included issuer costs related to authenticating the card and cardholder (such as PIN management and card-authentication technologies embedded in the card), providing alerts to cardholders about suspicious electronic debit transactions, receiving and processing reports of lost and stolen debit cards, reissuing debit cards used or suspected to have been used to make fraudulent electronic debit transactions, tracking and sharing information with payment card networks about compromised debit cards, monitoring compromised card databases, processing fraud claims and disputes of cardholders, activating cards, securing data systems, encrypting data, and ongoing research and development activities. Costs that were not included as part of the fraud-prevention adjustment included the cost of due diligence at account opening, the cost of routine mailings of newly issued or reissued cards, and the cost of fraud losses and any other costs allowed under the base interchange fee standard.

The adjustment amount in the interim final rule corresponds to the reported fraud-prevention costs, excluding those fraud-prevention costs included in the interchange fee standards in § 253.3, of the issuer at the median of the survey respondents. The median issuer's 2009 per-transaction fraud-prevention cost reported to the Board was 1.8 cents. The costs associated with research and development, card-activation systems, PIN customization, merchant blocking, and card-authentication systems were all small when measured on a per-transaction basis, typically less than one-tenth of a cent each. For all data-security costs reported by issuers in the card issuer survey, the median was 0.1 cents.

[21] 76 FR 43478, 43481 (Jul. 20, 2011).

In setting the interchange fee standard in § 235.3, the Board included costs of transaction-monitoring systems that are integral to the authorization of a transaction. Transaction monitoring systems assist in the authorization process by providing information to the issuer before the issuer decides to approve or decline the transaction. Because these costs are already included for all covered issuers as a basis for establishing the interchange fee standards, the Board excluded them in determining the fraud-prevention adjustment amount. The median issuer's transactions-monitoring cost is 0.7 cents per transaction. The fraud-prevention adjustment of 1 cent represents the difference between the median issuer's fraud-prevention cost of 1.8 cents per transaction less the median issuer's transaction-monitoring cost of 0.7 cents, rounded to the nearest cent.

B. Fraud-Prevention Costs Included in the Adjustment

1. Comments Received

In general, issuers and networks encouraged the Board to include costs of a broad set of fraud-prevention activities. In particular, these commenters recommended that the Board include in the calculation of the adjustment costs related to routine account monitoring, customer notifications, routine and non-routine card issuance and reissuance, name and address verification, chargeback costs, research and development of new fraud-prevention technologies, data security, card-activation systems, neural networks, transaction scoring, PIN customization, merchant blocking, other software systems, and lost revenue due to customers not having access to their debit card while awaiting reissuance. Some commenters encouraged the Board to include, in particular, the costs of activities undertaken in response to merchant data breaches.

Issuers also suggested that the Board include the costs of cardholder inquiries related to fraud, including providing payment transaction clarity so that customers are able to identify merchants listed on their statements. These commenters asserted that fraudulent transactions almost always involve a cardholder inquiry and that responding to cardholder inquiries is a fundamental and an economical means of preventing fraud as it permits issuers to gather information about lost and stolen cards, which is necessary to make decisions regarding appropriate responses to prevent fraud in connection with such cards. These commenters also noted that time and expense associated with cardholder inquiries is quantifiable and that the Board should try to determine the portion of cardholder inquiry costs related to fraud prevention.

A number of issuer commenters also encouraged the Board to base the fraud-prevention adjustment amount on the fraud-prevention costs of issuers that are exempt from the interchange fee standards in § 253.3 and the fraud-prevention adjustment in § 235.4.[22] Trade groups representing small issuers were concerned that the interchange fee standards, including the fraud-prevention adjustment, will become the *de facto* interchange fee level across the industry and that small issuers will suffer disproportionately because they tend to have higher per-transaction fraud-prevention costs.

Merchants, on the other hand, argued that the Board included too many fraud-prevention costs. One commenter asserted that including costs to detect and mitigate fraud goes beyond

[22] Institutions that have, together with their affiliates, assets of less than $10 billion are exempt from the interchange fee standards. 12 CFR § 235.5(a).

"preventing fraud." Additionally, merchants argued that the Board included costs of activities that have not been proven to prevent fraud, such as PIN customization (which one commenter argued makes PINs easier to guess) and research and development. Another commenter suggested that the Board more precisely delineate between activities that prevent fraud and those that do not.

Most merchant and merchant group commenters also asserted that the Board failed to take into account merchant's fraud-prevention costs, as required by EFTA Section 920(a)(5)(B). Several of these merchant commenters encouraged the Board to offset the adjustment amount by merchants' fraud-prevention costs or by the amount issuers recoup from other parties to the fraudulent electronic debit transaction through chargebacks or other means. One commenter argued that the desire to avoid or minimize the administrative burden associated with surveying merchants is not a sufficient reason for not measuring merchant costs. Another commenter argued that, by not considering specific merchants' fraud-prevention costs, merchants that have mostly card-not-present transactions essentially subsidize fraud prevention for the rest of the network, because those merchants tend to invest more in fraud prevention (to deal with higher rates of fraud in the card-not-present environment) than merchants that have mostly card-present transactions. One merchant commenter suggested that the Board take merchant costs into account by prohibiting issuers from imposing any fraud loss costs or PCI-DSS (or similar costs) on merchants if the fraud relates to transactions that qualify for the fraud-prevention adjustment.

2. Final Rule

Section 920(a)(5)(A)(i) of the EFTA permits the Board to allow an adjustment to the amount of an interchange fee that an issuer may receive or charge if "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." Fraud prevention involves a broad range of activities in which an issuer may engage before, during, or after an electronic debit transaction. Fraud-prevention activities include activities to detect fraudulent transactions. Detecting possible fraud during the authorization process, for example, can lead to actions such as denying a transaction or contacting the cardholder to verify the legitimacy of a previously authorized transaction. In this way, detecting possible fraudulent electronic debit transactions can prevent the fraud from happening. Similarly, issuers can take steps once fraud is discovered to mitigate the loss associated with the fraudulent activity. For example, an issuer may place an alert on a debit card indicating that the card or account information may have been compromised or cancel a compromised card and issue a new card to the cardholder in order to prevent future fraudulent transactions using the card. Thus, although the initial fraudulent transaction(s) may not have been prevented, an issuer can prevent additional fraud loss by taking such steps. Therefore, the Board has determined that activities that detect and mitigate fraudulent electronic debit transactions contribute to preventing fraud and that the costs of such activities are appropriate to include for purposes of the fraud-prevention adjustment.

Costs associated with research and development of new fraud-prevention technologies, card reissuance due to fraudulent activity, data security, card activation, and merchant blocking are all examples of costs that are incurred to detect and prevent fraudulent electronic debit transactions. Therefore, the Board has included the costs of these activities in setting the fraud-prevention adjustment amount to the extent the issuers reported these costs in response to the

survey on 2009 costs. As in the interim final rule, the Board has determined to exclude from the adjustment amount any costs included in the interchange fee standards in § 253.3. Thus, the costs of transaction monitoring activities such as the use of neural networks and transactions scoring systems that assist in the authorization process by providing information to the issuer before the issuer decides to approve or decline the transaction were not considered.

Section 920(a)(5) allows the Board to permit an adjustment to make allowance for costs incurred by the issuer in preventing fraud in relation to electronic debit transactions. Accordingly, the Board did not include costs incurred to prevent fraud to a cardholder's transaction account through means other than fraudulent electronic debit transactions, or costs incurred to prevent fraud in connection with other payment methods such as credit cards. For example, name and address verification used in opening a checking account is an excluded activity because it involves preventing fraud with respect to the entire account relationship and is performed whether or not a debit card is issued as a means of making payments from the account. Similarly, the costs of activities employed solely to prevent fraudulent credit card transactions are not included. To the extent an issuer engages in an activity or activities to prevent both fraudulent credit card and debit card transactions (e.g., securing data across all of its card programs), issuers were instructed to allocate such joint costs in the issuer survey based on the relative proportion of the cost of the activity that was tied to debit card transactions, and only that proportion of costs was included in determining the fraud-prevention adjustment.

Additionally, fraud losses, including ATM losses, and the lost revenue due to customers' inability to use their debit cards while awaiting reissuance are not costs incurred to prevent fraudulent electronic debit transactions and are excluded. Similarly, costs of purchasing fraud-loss insurance or recovering losses also are excluded as these are not costs incurred to prevent fraudulent electronic debit transactions.

Fraud-prevention costs of exempt issuers. EFTA Section 920(a)(6)(A) provides an exemption from EFTA Section 920(a) for any issuer that, together with its affiliates, has assets of less than $10 billion. EFTA, however, does not provide the Board with specific authority to require networks to implement these exemptions in any particular way. The Board recognizes the concerns raised by small issuers that market forces could lead to a convergence of the interchange fee levels of exempt and nonexempt issuers and that small issuers could suffer disproportionately because they tend to have higher per-transaction fraud-prevention costs. Nonetheless, the Board's interchange fee standard, including the fraud-prevention adjustment, does not itself limit the amount of interchange fees small issuers may receive or charge. Moreover, the Board recognizes that requesting that small issuers record and report their costs associated with authorizing, clearing, and settling electronic debit transactions and the costs associated with fraud prevention and data security would impose administrative burden on these entities. Therefore, the Board has determined not to include in the adjustment the fraud-prevention costs incurred by small issuers. As noted in the preamble to the Board's final rule implementing other provisions of EFTA Section 920, the Board is monitoring the effectiveness of the exemption for small issuers and notes that, in the fourth quarter of 2011, the first quarter during which the interchange fee standards went into effect, nearly all payment card networks

offered small issuers a higher interchange fee than that set forth in the standards and that the average interchange fee for small issuers is about the same as it was for all issuers in 2009.[23]

Fraud-prevention costs incurred by other parties. EFTA Section 920(a)(5)(B)(ii) requires the Board to consider the fraud-prevention and data-security costs expended by each party involved in electronic debit transactions. The Board recognizes that all parties to electronic debit transactions, including merchants, incur fraud-prevention costs. For example, both merchants and issuers incur costs to comply with PCI-DSS and network rules related to fraud prevention. Moreover, certain merchants, such as Internet merchants, have developed customized approaches to prevent fraud and secure customer data in response the particular fraud risks faced in their sales environments.

The Board has given consideration to, and taken into account, the fraud-prevention costs of other parties by setting the adjustment based on the costs of the median issuer (as opposed to the interchange fee standards in § 253.3, which were set at the 80th percentile issuer).[24] This lower amount is intended, in part, to reduce the adjustment as a way to recognize the fraud-prevention and data-security costs of merchants and parallels the *ad valorem* component of the base interchange fee standard (5 basis points multiplied by the transaction value), which was set at the median issuer's per-transaction fraud losses. Further, as discussed in connection with the Board's fraud-prevention standards in § 235.4(b), the Board also is requiring issuers to take into account whether, and to what extent, fraud-prevention technologies implemented by an issuer are likely to impose costs on other parties. Requiring an issuer to take into account the costs borne by other parties in these ways obviates the need to impose a burdensome survey on merchants and other parties about their fraud-prevention costs.

C. Adjustment Amount

1. Comments Received

The maximum permissible fraud-prevention adjustment amount in the interim final rule is 1 cent. In general, issuers, depository industry trade associations, and payment card networks supported increasing the adjustment amount and asserted that the adjustment amount in the interim final rule would discourage innovation and investment in fraud-prevention activities, particularly in technology requiring substantial upfront investment. Issuers also argued that the 1-cent adjustment amount would undermine the goal of protecting cardholder financial information. Another commenter stated that an insufficient fraud-prevention adjustment could lead to an increase in declined transactions at the point of sale as issuers become more conservative in transaction authorizations. Another issuer commenter believed that the fraud-prevention adjustment disproportionately shifts the burden on issuers to implement fraud-prevention measures without reasonable compensation.

[23] 76 FR 43394, 43436 (Jul. 20, 2011). See http://www.federalreserve.gov/paymentsystems/regii-average-interchange-fee.htm.
[24] 76 FR 43394, 43433-34 (Jul. 20, 2011).

Several issuers suggested setting the adjustment amount based on the costs of the issuer at the 80th percentile, consistent with the interchange fee standards in § 235.3. Issuer commenters stated that the Board provided no explanation for setting the adjustment at the median while the interchange fee standard was set at the 80th percentile of issuers' reported costs or for why the fraud-prevention activities of issuers with costs above the median were not viewed as cost-effective.

A few issuers suggested incorporating an *ad valorem* component because issuers often target their fraud-prevention investments at large-value transactions. One issuer suggested that an *ad valorem* component also could vary based on the type of merchant in order to compensate issuers for fraud-prevention costs associated with riskier merchants.

Other comments from issuers suggested other manners in which the fraud-prevention amount could vary. Specifically, one issuer suggested increasing the adjustment amount for those issuers with higher-than-average fraud losses because such issuers will both absorb more fraud losses and incur more costs to prevent and mitigate fraud. Another issuer suggested imposing a higher fraud-prevention adjustment on merchants that are not PCI-DSS compliant or to set the fraud-prevention adjustment amount as a percentage of interchange fee revenue.[25] One issuer group suggested varying the fraud-prevention adjustment based on the charge-back rate of the merchant involved in the transaction.

One technology company suggested that issuers receive an additional amount for adopting specific fraud-prevention technologies such as biometric facial recognition software or other authentication methods not yet prevalent in the industry.

In general, merchants and their associations urged the Board to adopt a lower adjustment amount. Some merchant groups opposed the use of the data collected from issuers to determine the amount of the adjustment, arguing that the survey was flawed. These commenters argued that the Board did not reveal results from the survey until it published the interim final rule, that only a small subset of covered issuers responded, and that there was no independent verification. One merchant commenter supported the adjustment amount in recognition of the fact that issuers ultimately are subject to complying with the Board's fraud-prevention standards, but opposed the Board increasing the adjustment amount higher than 1 cent. One merchant questioned whether a fraud-prevention adjustment was necessary given the amount an issuer could receive or charge under the base interchange fee standard.

2. Final Rule

The Board has considered the comments and has determined to retain the 1-cent fraud-prevention adjustment amount that is permitted in the interim final rule. As mentioned above, the Board initially set the adjustment amount at the fraud-prevention cost of the median issuer based on 2009 fraud-prevention costs reported by issuers in response to the Board's 2010 survey, minus those fraud-prevention costs that are already part of the interchange fee standards in § 253.3. The Board chose to set the adjustment based on the median cost to balance the fraud-prevention and data-security costs incurred by issuers and those incurred by merchants, some of

[25] This commenter suggested that the percentage be set at 19 percent, which the commenter estimated to be issuers' historic fraud-prevention costs as a percentage of historic interchange fee revenue.

which are incurred due to the fraud-prevention methods selected by issuers. This consideration and approach parallels the approach taken with respect to the *ad valorem* component of the base interchange fee standard. The *ad valorem* component, which accounts for fraud losses incurred by issuers, was set at the median issuer's fraud losses (i.e., 5 basis points multiplied by the transaction value). In setting the *ad valorem* component, the Board explicitly recognized that both issuers and merchants incur fraud losses.[26]

The Board has considered the comments suggesting an *ad valorem* component and has determined not to include such a component in the fraud-prevention adjustment amount. An *ad valorem* component is more appropriate for measuring fraud losses, for which there is a direct correlation between transaction value and the amount of the loss, than when measuring fraud-prevention costs, which may, but do not necessarily, vary with the value of a transaction. The Board notes that the 1-cent adjustment does not limit a payment card network's ability to vary the overall interchange fee rate based on the type of merchant, for any of the aforementioned reasons, so long as an issuer does not receive interchange fees, including the fraud-prevention adjustment, greater than permitted in Regulation II.

The Board has also determined not to permit issuers to receive or charge an adjustment above the 1-cent amount for adopting certain new authentication methods. As noted below in connection with § 235.4(b), the Board has taken a non-prescriptive approach to allow for flexibility in using a variety of methods to prevent fraudulent electronic debit transactions.

As previously noted, the Board is using the fraud-prevention cost data as reported by issuers for 2009 in determining the maximum fraud-prevention adjustment amount permitted in Regulation II. Since that time, the Board has surveyed issuers that are not exempt from the interchange fee standards for their data for calendar year 2011. At the time of this final rule, the Board is still processing and analyzing the 2011 data. The Board will take into account data from the 2011 survey and future surveys when considering any future revisions to the fraud-prevention adjustment.

D. Application to All Transactions

1. Comments Received

The interim final rule permits an issuer to receive or charge the fraud-prevention amount for all types of electronic debit transactions. Several merchant commenters encouraged the Board to permit an adjustment only for PIN-based transactions, due to the lower fraud rates of PIN-based debit compared to signature-based debit. Other merchant commenters suggested the Board permit an adjustment only for authentication methods that have fraud rates demonstratively lower than those for PIN transactions. One individual suggested that the Board provide greater disincentives, such as a negative adjustment, for less secure technologies and asserted that doing so was consistent with the statutory directive to consider the extent to which the occurrence of fraud depended on the authentication method.

Issuers and networks supported applying the adjustment to all debit card transactions. These commenters argued that not all authentication methods are available for all transactions.

[26] 76 FR 43394, 43434 (Jul. 20, 2011).

One consequence of this, they argued, is that lower fraud rates and losses for PIN may be due to the fact that signature is the only method available for Internet transactions and that PIN fraud, unlike signature fraud, often manifests itself as ATM fraud, which the Board did not take into account. Some of these commenters also argued that limiting the adjustment to PIN transactions would create disincentives to invest in signature and other non-PIN based fraud prevention. Authentication technology providers also supported not limiting the adjustment to authentication methods that exist and are used widely today.

2. Final Rule

The Board has considered the comments and has determined that an eligible issuer may receive or charge a fraud-prevention adjustment for all electronic debit transactions irrespective of the authentication method used for the transaction. As recognized in the interim final rule, limiting the adjustment to only a subset of authentication methods, or only those available today, may not provide issuers with sufficient flexibility to develop other methods of authentication that may be more effective than today's alternatives and may not require a PIN. Limiting the transactions eligible for a fraud-prevention adjustment also may reduce the incentives for issuers to improve fraud-prevention techniques for authentication methods that, for a variety of reasons, experience higher fraud rates. Further, because issuers are less likely to receive a higher interchange fee for signature-based transactions than in the past, the Board believes that issuers' incentives to encourage cardholders to use their signature rather than their PIN to authenticate transactions at the point of sale will diminish.

II. Section 235.4(b)(1) Issuer fraud-prevention standards

A. Proposed Rule and Interim Final Rule

The Board's 2010 proposed rule did not contain a specific proposal for a fraud-prevention adjustment to the interchange fee standards. Instead, as discussed above, the Board requested comment on two general approaches to an adjustment: a technology-specific approach, which would permit an issuer to recover costs for major innovations identified by the Board as likely to result in substantial reductions in fraud losses, and a non-prescriptive approach, which would involve more general standards for an issuer to satisfy without the prescription of specific technologies.[27] With respect to that initial proposal, commenters generally opposed the Board mandating specific technologies for many reasons, including that a technology-specific approach would not necessarily be more effective than an approach that involves a variety of technologies, practices, and methods and that a technology-specific approach could deter investment in new technologies.

Issuers, depository institution trade associations, and payment card networks preferred the non-prescriptive approach because that approach would maintain issuer flexibility to respond to existing and emerging fraud risks and to do so in a timely manner. Merchants supported an approach that provided incentives to issuers and networks to switch from the current methods and technologies to more effective ("paradigm shifting") fraud-prevention technologies. One merchant group's suggestion, supported by many other merchant commenters, proposed an

[27] For a more detailed description of the two approaches proposed by the Board, see 75 FR 81722, 81742-43 (Dec. 28, 2010).

approach under which any technologies issuers wanted to offer to merchants must undergo an application and approval process managed by the Board before the issuer would be eligible to receive the fraud-prevention adjustment. This merchant group suggested that, as part of the application and approval process, an issuer must demonstrate that the technology reduces fraud to a level materially lower than that associated with PIN debit transactions.[28]

The Board adopted the non-prescriptive approach to fraud-prevention standards in the interim final rule. The Board determined that the dynamic nature of the debit card fraud environment necessitates standards that permit issuers to identify the best methods to detect, prevent, and mitigate fraud losses for the size and scope of their debit card programs and to respond to frequent changes in fraud patterns. In addition, specifying and limiting the set of technologies for which issuers recover their costs may weaken the long-term effectiveness of the specified technologies. The reasons for selecting the non-prescriptive approach for the interim final rule are set forth more fully in the *Federal Register* notice announcing the interim final rule.[29]

Section 235.4(b)(1) of the interim final rule requires an issuer, in order to be eligible to receive a fraud-prevention adjustment, to develop and implement policies and procedures reasonably designed to: (1) identify and prevent fraudulent electronic debit transactions; (2) monitor the incidence of, reimbursements received for, and losses incurred from fraudulent electronic debit transactions; (3) 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 (4) secure debit card and cardholder data. Procedures could include practices, activities, methods, or technologies that are used to implement and make effective an institution's fraud-prevention policies. The commentary to § 235.4(b) discusses the types of fraud that an issuer's policies and procedures should address, which includes the unauthorized use of a debit card (*see* interim final rule comment 4(b)-2). The commentary to the interim final rule also provides examples of practices that may be part of an issuer's policies and procedures that are reasonably designed to achieve each of the fraud-prevention goals in § 235.4(b)(1).[30] The commentary to the interim final rule, and changes thereto, are discussed below more fully in connection with the applicable fraud-prevention objective set forth in § 235.4(b).

B. Comments Received

Issuers and networks overwhelmingly supported the non-prescriptive framework and standards in § 235.4(b). Issuers and networks asserted that the non-prescriptive approach would provide incentives to prevent fraud and invest in new fraud-prevention technologies, while also providing flexibility for each issuer to determine its optimal fraud-prevention solutions (including non-technology based solutions) and enabling issuers, networks, and acquirers to compete based on fraud-prevention tools. Issuers and networks opposed a technology-specific approach, which they argued would lock the industry into particular technologies, give fraudsters advance notice of fraud-prevention methods, slow the implementation of new technology, and

[28] *See* comment letter on the proposed rule from the Merchants Payments Coalition and comment letter on the interim final rule from the Merchants Payments Coalition.
[29] 76 FR 43394, 43478 (Jul. 20, 2011).
[30] *See* interim final rule comments 4(b)(1)(i) through 4(b)(1)(iv) in Appendix A to 12 CFR part 235.

result in an inefficient allocation of resources by discouraging new investments in other technologies. Moreover, issuers and networks did not believe that the government was better positioned than industry participants to select the most effective and commercially feasible fraud-prevention technology.

Merchants opposed both specifying particular fraud-prevention technologies in the rule (although supported Board-involvement in approving eligible technologies) and the standards as set forth in the interim final rule. Many merchants opposed the standards in the interim final rule because they believed that the standards, as drafted, would permit issuers to qualify for an adjustment by adopting existing fraud-prevention technologies, which the merchant commenters believed to be ineffective at preventing fraud. In addition, one merchant believed that the standards were too vague and may inadvertently lead to issuers adopting policies and procedures that are inconsistent with providing economical means of reducing fraud. Merchants restated their support for the paradigm-shifting approach suggested in response to the proposed rule in which an issuer would be eligible for the fraud-prevention adjustment only if the issuer adopted a technology that reduced fraud to levels that are materially lower than the levels experienced with PIN debit, and only after the issuer documented the technology's effectiveness and cost-effectiveness to the Board.[31] The approach proposed by merchants also would require the Board to request public comment on the effectiveness and cost-effectiveness of fraud-prevention technologies and formally approve particular technologies prior to an issuer being able to receive a fraud-prevention adjustment for transactions that use the technology. One merchant commenter supported an alternative approach under which issuers, not networks, would offer technologies to merchants and merchants would determine which issuers' solutions to implement based on the solution's cost and effectiveness.

Issuers widely supported the Board's standards in the interim final rule and argued that they should be eligible for the adjustment without demonstrating actual reductions in fraud because fraud may be caused by factors outside of the issuer's control. By contrast, merchants and their trade groups believed the standards to be inconsistent with EFTA Section 920(a)(5)'s requirements. Specifically, merchants argued that the standards should require an issuer to demonstrate quantifiable reductions in the incidence of fraud prior to receiving a fraud-prevention adjustment. One merchant commenter argued that requiring issuers' policies and procedures to be "reasonably designed" to achieve the Board's objectives is not equivalent to requiring issuers to take "effective" steps to prevent fraud, which is the requirement in EFTA Section 920(a)(5).[32]

Merchant commenters, as well as a member of Congress, encouraged the Board to adopt metrics-based standards to ensure that issuers receive the fraud-prevention adjustment only if they reduce fraud losses or the occurrence of fraud to specified levels, for example, at or below the industry fraud levels for PIN debit transactions. This approach, the commenters argued, would ensure that the market has proper incentives to adopt effective fraud-prevention technology.

---

[31] One commenter was indifferent between the two approaches provided Board does not prescribe how merchants must implement fraud-prevention technologies.

[32] One commenter was concerned that the rule does not appear to require that the issuer actually adhere to the policies and procedures prior to receiving an adjustment. The interim final rule requires that an issuer implement the policies and procedures in addition to developing the policies and procedures.

Merchants also argued that the Board's standards were inconsistent with EFTA Section 920(a)(5)'s requirement that issuers develop and implement cost-effective fraud-prevention technology. Merchants argued that the Board's standards failed to demonstrate the cost-effectiveness of fraud-prevention measures. One merchant group believed that the cost-effective requirement could be satisfied only if the adjustment is based on issuer-specific fraud reduction and cost. By contrast, one issuer argued that whether or not a fraud-prevention activity is "cost-effective" may not be apparent at the outset, because new fraud-prevention activities must be monitored over time to assess cost-effectiveness. This issuer suggested that the Board continue gathering additional information about issuers' costs for new fraud-prevention activity.

Finally, merchants argued that the Board's standards do not require an issuer receiving the adjustment to demonstrate that it has made any investments in fraud-prevention activities that reduce fraud.

C. Non-prescriptive Standards

The Board has considered the comments and has adopted fraud-prevention standards in the final rule that largely follow the non-prescriptive approach set forth in the interim final rule. The Board has revised § 235.4(b)(1) to provide that, in order to be eligible for a fraud-prevention adjustment to the amount of any interchange fee received or charged in accordance with § 235.3, an issuer must develop and implement policies and procedures reasonably designed to take effective steps to reduce the occurrence of, and costs to all parties from, fraudulent electronic debit transactions, including through the development and implementation of cost-effective fraud-prevention technologies. New § 235.4(b)(2) will continue to require an issuer's policies and procedures to address fraud-prevention objectives similar to those in the interim final rule (discussed further below), but the Board is expanding the scope of those policies and procedures to permit issuers to consider factors other than those explicitly listed, if appropriate.

After considering the comments received, the Board has determined that the final rule should not prescribe specific technologies that an issuer must implement in order to be eligible to receive an adjustment. The dynamic nature of the debit card fraud environment and the variation in issuer debit card portfolios, customer base, and transaction-processing arrangements requires standards that permit issuers to determine the best methods to detect and prevent fraudulent transactions, and mitigate fraud losses from those transactions, as well as to respond to the frequent changes in industry fraud types and methods, and available fraud-prevention methods. Standards that incorporate a technology-specific approach would not provide issuers with sufficient flexibility to design and modify policies and procedures that best meet a particular issuer's needs and that most effectively reduce fraud losses to all parties involved in the transactions.

Similarly, standards that restrict eligible fraud-prevention technologies to those that an issuer has demonstrated to be effective and that have been subject to a Board approval process would not provide sufficient flexibility to issuers. Moreover, because existing fraud-prevention technologies are implemented as part of broader fraud-prevention programs, requiring issuers to isolate and measure the effectiveness of a particular fraud-prevention technology would be impractical.

Prescribing one eligible technology or a limited set of eligible technologies also could inhibit investment in new, "non-eligible" technologies (i.e., those for which effectiveness has not yet been demonstrated because they are not implemented in the marketplace), which ultimately could become more effective than "eligible" technologies. Specifically prescribing eligible fraud-prevention technologies also would provide fraudsters with information on the fraud-prevention technologies prevalent in the industry, which could make those technologies less effective over time.

Moreover, even the most effective fraud-prevention technologies issuers could implement would not prevent all fraudulent electronic debit transactions. This fact underscores the need for a fraud-prevention program that also involves non-technology-based policies and procedures (such as notifying customers of potentially fraudulent transactions) that complement technology-based fraud-prevention solutions.

D. Fraudulent Electronic Debit Transactions

In its proposed rule, the Board did not include a definition of "fraud" or "fraudulent electronic debit transaction," but 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."[33] The Board noted that this definition was derived from the EFTA's definition of "unauthorized electronic fund transfer."[34] After considering the comments received on the proposed rule, the Board determined that fraud is broader than unauthorized use and that whether a transaction is fraudulent depends on the facts and circumstances.[35] Accordingly, the Board did not include a regulatory definition of "fraudulent electronic debit transaction" in the interim final rule. Instead, the Board provided three examples in the interim final rule's comment 4(b)-2 of the types of fraud that an issuer's policies and procedures should address: (1) a person uses a stolen debit card to make an unauthorized purchase; (2) a merchant uses cardholder information from a previous transaction to make a subsequent, unauthorized transaction; and (3) a hacker obtains card information and uses that information to make an unauthorized purchase. The Board requested comment on whether the rule should include a definition of "fraud" or "fraudulent electronic debit transaction," and if so, what would be an appropriate definition.

Commenters were divided as to whether the Board should define "fraud" or "fraudulent electronic debit transaction" in the regulatory text. Some issuers opposed defining either term because fraud is constantly changing and defining the term in the regulatory text would provide issuers with less flexibility to adapt their fraud-prevention programs to changing fraud. Other issuers opposed including a definition arguing that what is fraud is a judicial concept that should not be defined in the regulatory text. In general, commenters that supported including a definition of "fraud" or "fraudulent electronic debit transaction" appeared to do so as a means to

[33] *See* 75 FR 81722, 81740 (Dec. 28, 2010).
[34] 15 U.S.C. § 1693a(11).
[35] In announcing the interim final rule the Board noted that fraud could include, for example, a situation where a cardholder authorizes a transaction, but either the merchant is fraudulent and does not deliver the expected goods or services or the cardholder fraudulently alleges that he or she never received the goods or services. *See* 76 FR 43478, 43485 (Jul. 20, 2011).

either limit or expand the types of fraud-prevention activities an issuer's policies and procedures should address.[36]

Commenters that supported including a definition of "fraud" or "fraudulent electronic debit transaction" in the regulatory text were divided as to how the Board should define any such term. One merchant commenter suggested that the definition be limited to the unauthorized use of the debit card in order to exclude transactions by fraudulent merchants and fraudulent cardholders, such as those who legitimately own the card but are using it to commit fraud. One issuer suggested defining "fraudulent electronic debit transaction" as including both the unauthorized use of a debit card from which the cardholder receives no benefit and the use of a debit card by a cardholder, or person acting in concert with a cardholder, with fraudulent intent. Some issuers suggested that the definition include ATM fraud losses because often these losses are a result of security breaches at the point of sale. One depository institution trade group, while not commenting explicitly on the appropriateness of a regulatory definition, opposed the commentary's examples of fraudulent debit card transactions, because the commenter believed that by including the examples, the Board was suggesting that issuers were the appropriate party to prevent the fraud in each example, even though the merchant may be in the best position to prevent fraud in the examples provided.

The final rule does not include a regulatory definition of either "fraud" or "fraudulent electronic debit transaction." The Board continues to believe that which transactions are considered fraudulent will be determined based on the facts and circumstances and may evolve over time. The Board also continues to believe that fraudulent electronic debit transactions should not be limited to the "unauthorized" use of a debit card, as that term is used elsewhere in the EFTA, because all types of fraud impose costs on system participants. Accordingly, an issuer's policies and procedures should be designed to reduce the occurrence of, and costs to all parties from, all types of fraud and not merely the unauthorized use of a debit card.

The Board, however, has made clarifying changes to interim final rule comment 4(b)-2, which is redesignated as comment 4(b)(1)-1 (hereinafter referred to as comment 4(b)(1)-1). In the interim final rule, the comment provided that the listed examples of fraud are types of fraud that could be "effectively addressed by the issuer, as the entity with the direct relationship with the cardholder and that authorizes the transaction." The Board recognizes that in some instances the issuer may be able to use its direct relationship with the cardholder to prevent these types of fraud (e.g., through comparing the unauthorized transaction to its cardholder's typical transaction pattern). Although an issuer may be unable to effectively address all of these types of fraud in all situations, an issuer should be able to develop and implement policies and procedures designed to detect and prevent fraudulent transactions of the types listed. For example, an issuer could develop and implement policies and procedures to deactivate a card upon notice that the card has been stolen. Therefore, the Board is removing from comment 4(b)(1)-1 the statement that the examples correspond to the types of fraud that an issuer can prevent. The Board also has revised that comment to clarify that the types of fraud an issuer's policies and procedures should address are not limited to those included in the examples. The Board also made other minor editorial changes to this comment.

[36] One issuer suggested that any definition of "fraud" or "fraudulent electronic debit transaction" be silent on any authentication method that must be used so that issuers have flexibility in preventing fraud.

E. Policies and Procedures Designed to Take Effective Steps

Section 920(a)(5) of the EFTA mandates that the Board's fraud-prevention standards require an issuer 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 technologies. In assessing whether an issuer is taking effective steps to reduce fraudulent electronic debit transactions, the Board does not believe that Section 920(a)(5) requires that the steps an issuer takes prevent all fraud. Moreover, the Board does not believe, as some merchant commenters argued, that an issuer be required to demonstrate that a particular fraud-prevention measure directly led to a reduction in fraudulent electronic debit transactions before the cost of that measure is included in the fraud-prevention adjustment. Isolating the effectiveness of a particular fraud-prevention measure is virtually impossible due to the numerous fraud-prevention methods and technologies implemented by an issuer and the fact that the effectiveness of a particular measure may not be evident until a year or more after implementation. In addition, an issuer's incidence of fraudulent electronic debit transactions may fluctuate for various reasons, including factors outside the issuer's control (e.g., a data breach at a large merchant processor).

EFTA Section 920(a)(5) requires that an issuer take effective steps to reduce fraudulent electronic debit transactions, without any reference to the size of the reduction. The language of EFTA Section 920(a)(5) does not compel the Board to impose a maximum permissible level of fraudulent electronic debit transactions for an issuer to be eligible to receive a fraud-prevention adjustment. In addition, selecting a benchmark fraud level would not necessarily ensure that issuers continue to take effective steps to reduce fraudulent transactions due to the variety of sales channels and evolving fraud-prevention technologies. An issuer may not have incentives to develop or invest in new and potentially more effective fraud-prevention technologies for sales channels that experience fraud levels below the selected benchmark level or if the issuer experiences fraud at a level below the selected benchmark. Moreover, deeming an issuer to be eligible for an adjustment if the issuer's fraud rate is below some industry rate would not necessarily satisfy the requirement that the Board's standards require an issuer to take effective steps to reduce the occurrence of, and costs to all parties from, fraudulent electronic debit transactions involving that issuer. For example, an issuer with a fraud rate significantly below the benchmark may be able to qualify for a fraud-prevention adjustment even if the steps that issuer is taking are no longer effective in *reducing* the occurrence of, and costs from, fraud in relation to electronic debit transactions involving that issuer.

In addition, requiring issuers to maintain fraud below a benchmark level, particularly one based on technology that may not be available widely for all point-of-sale channels, could have adverse consequences for consumers. Cardholders may not always be able to use lower-fraud fraud-prevention methods (such as PIN) in all point-of-sales channels.[37] Issuers may, for example, set more restrictive authorization rules for transactions in the sales channels for which the benchmarked cardholder-authentication technology is not available.

[37] For example, while the Board understands that technology is developing to allow PIN debit transactions for Internet transactions, this technology is not widely used.

The final rule permits an issuer to receive the fraud-prevention adjustment if it develops and implements policies and procedures reasonably designed to take effective steps to reduce the occurrence of, and costs to all parties from, fraudulent electronic debit transactions and if those policies and procedures address the fraud-prevention aspects in revised § 235.4(b)(2). This approach recognizes that, at the outset, an issuer cannot predict with certainty that any particular policies and procedures will effectively prevent fraud in relation to electronic debit transactions. The Board believes that providing specific factors that issuers must address in their policies and procedures, but providing flexibility in how those policies and procedures may be implemented to address those factors, over time will allow for more effective fraud prevention. This approach permits issuers to adjust their practices based on new fraud-prevention technologies and practices, new patterns of fraud, changes to the size of their debit card programs, and changes in how their customers use debit cards. (*See* discussion below of § 235.4(b)(2) and commentary.) Under the final rule, an issuer must be able to demonstrate that its policies and procedures are reasonably designed to take effective steps to reduce fraudulent electronic debit transactions.

The Board has added new comment 4(b)(1)-2 to clarify that an issuer's policies and procedures must be designed to reduce fraud, where cost-effective, across all types of electronic debit transactions in which its cardholders engage.[38] An issuer may enable multiple types of card-authentication methods on its debit cards (e.g., a chip or a code embedded in the magnetic stripe) as well as permit multiple cardholder-authentication methods (e.g., a signature or a PIN). Accordingly, the Board believes that an issuer should consider whether its fraud-prevention policies and procedures are effective for each method used to authenticate the card and the cardholder. In addition, the effectiveness of the card- and cardholder-authentication methods an issuer has enabled on its debit cards likely will vary based on the sales channel in which the debit card is used. For example, in a card-not-present environment (e.g., the Internet), a chip or a code embedded in the magnetic strip may not be used to authenticate the card. Therefore, new comment 4(b)-2 provides that an issuer should consider the effectiveness of its fraud-prevention policies and procedures for different sales channels for which the card is used (e.g., card-present and card-not-present).

The Board has not adopted the language in interim final rule comment 4(b)(1)(i)-2 requiring an issuer to consider practices to encourage its cardholders to use the materially more effective authentication method and to consider methods for reducing fraud for the less effective authentication method. Since October 1, 2011, when the Board's interchange fee standards became effective, the differential in interchange fee revenue across networks supporting different authentication methods largely has been eliminated for issuers that are subject to the interchange fee standards. Accordingly, issuers no longer have the incentive to steer cardholders to one type of authentication method over another. Issuers, however, will continue to be required to review the effectiveness of each of their authentication methods as part of the required review of their fraud-prevention policies and procedures.

Relatedly, the Board requested comment on whether the Board's standards 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. A few issuers opposed requiring issuers to assess customer rewards policies because

[38] Comment 4(b)-5, discussed below, describes the cost-effective aspect in more detail.

doing so was outside the Board's authority and unnecessary. Specifically, these issuers believed that the interchange fee standards in § 235.3 likely would reduce the prevalence of reward programs. In addition, issuers argued that they consider a variety of factors when determining whether to offer rewards programs and expressed confusion as to what would constitute an "inappropriate incentive." One merchant trade group supported prohibiting issuers from receiving a fraud-prevention adjustment if they provide incentives to use a high-fraud authentication method, and one consumer group supported a requirement on issuers to assess whether their rewards programs are encouraging the use of less secure fraud-prevention technologies.

For reasons similar to the determination not to adopt the language in interim final rule comment 4(b)(1)(i)-2, the Board has neither imposed a specific requirement that issuers assess whether their rewards programs provide incentives to cardholders to use higher-fraud authentication methods nor prohibited issuers from receiving a fraud-prevention adjustment due to their use of rewards and other incentives. Issuers offer rewards programs to cardholders for a variety of reasons, and, to the extent rewards programs were based on differentials in interchange fees across networks, § 235.3 effectively has largely eliminated a covered issuer's incentive to offer rewards for transactions over one network. Accordingly, the potential fraud-prevention benefit from explicitly requiring issuers to assess whether cardholder rewards or similar incentive programs provide an inappropriate incentive to use higher-fraud authentication methods is significantly outweighed by the added burden that would be imposed on issuers.

EFTA Section 920(a)(5) also provides that an issuer must take effective steps to reduce "costs from" fraudulent electronic debit transactions.[39] EFTA Section 920(a)(5)(A)(i)(II) is silent as to which parties' costs the Board's standards must ensure that an issuer take effective steps to reduce. EFTA Section 920(a)(5)(B)(ii), however, explicitly requires the Board to consider the costs of fraudulent transactions absorbed by each party involved in such transactions. As a result of various laws, regulations, and payment card network rules (discussed above) that allocate the costs of fraudulent electronic debit transactions among different parties to the fraudulent transactions, issuers, acquirers, and merchants typically all absorb losses from fraudulent electronic debit transactions.[40] The Board believes that an issuer should take effective steps to reduce costs from fraudulent transactions that are incurred by all parties to such transactions, and not merely steps that reduce the issuer's own fraud losses. Accordingly, the Board is providing in revised § 235.4(b) that an issuer must reasonably design its policies and procedures "to take effective steps to reduce the occurrence of, *and costs to all parties from,* fraudulent electronic debit transactions" (emphasis added).

New comment 4(b)-3 provides guidance on the reduction in the occurrence of, and costs to all parties from, fraudulent electronic debit transactions. A reduction in the occurrence of fraudulent electronic debit transactions can be measured by determining whether there is a reduction in the number of an issuer's electronic debit transactions that are fraudulent relative to the issuer's total electronic debit transactions. The Board believes that measuring a reduction in the occurrence of fraudulent electronic debit transactions in relation to an issuer's total

[39] EFTA Section 920(a)(5)(A)(i)(II).

[40] Most issuers indicated that they impose zero liability on their cardholders for fraudulent transactions, and most acquirers reported limited fraud losses, indicating that merchant acquirers pass through fraud losses to merchants.

transactions is more appropriate than measuring the reduction in terms of the absolute number of fraudulent transactions. Measuring only the change in the number of an issuer's fraudulent electronic debit transactions would not, for example, account for an increase in the number of electronic debit transactions initiated by an issuer's cardholders. In addition, an issuer must implement policies and procedures that are reasonably designed to reduce the value of its electronic debit transactions that are fraudulent relative to non-fraudulent transactions. New comment 4(b)-3 emphasizes that an issuer's policies and procedures should be reasonably designed to reduce the costs of fraudulent transactions to all parties, irrespective of whether the issuer ultimately bears the fraud losses as a result of regulations or network rules.

New comment 4(b)-4 recognizes that the number and value of an issuer's fraudulent electronic debit transactions relative to non-fraudulent transactions may vary materially from year to year and that, in certain circumstances, an issuer's policies and procedures may be effective notwithstanding a relative increase in transactions that are fraudulent in a particular year. For example, a data breach at a merchant processor that exposes the data of a substantial portion of an issuer's cards and cardholders could result in the issuer having a relatively higher number of fraudulent transactions in one year than in the preceding year, even if the issuer had implemented the same or improved fraud-prevention policies and procedures. This could be a circumstance in which an issuer's policies and procedures may be effective notwithstanding a relative increase in transactions that are fraudulent.

Continuing increases in an issuer's fraudulent transactions relative to non-fraudulent transactions, however, would warrant further scrutiny as to the effectiveness of an issuer's policies and procedures. For example, instead of at a merchant processor, the data breach might occur at the issuer or the issuer's processor. As a result, an issuer may experience higher fraud rates in one year and, in the following years, the share of that issuer's transactions that are fraudulent may continue to increase. Further scrutiny would be warranted to determine, for example, whether the issuer's policies and procedures are designed to take effective steps to prevent fraudulent transactions as a direct result of the initial data breach and to prevent subsequent data breaches from occurring.

F. Development and Implementation of Cost-effective Technologies

EFTA Section 920(a)(5) states that the Board's fraud-prevention standards must require an issuer to take effective steps to reduce the occurrence of, and costs from, fraudulent electronic debit transactions, including through the development and implementation of cost-effective fraud-prevention technologies. Some merchant commenters argued that the Board's standards in the interim final rule failed to require issuers to demonstrate the cost-effectiveness, particularly vis-à-vis merchants, of their fraud-prevention measures prior to receiving the fraud-prevention adjustment. One commenter believed that the Board's standards could not satisfy the cost-effective requirement in the statute unless the adjustment amount is based on issuer-specific fraud reduction and cost. By contrast, one issuer asserted that measuring the cost-effectiveness

of a particular activity at the outset may not be possible because new fraud-prevention activities must be monitored over time to assess cost-effectiveness.[41]

EFTA Section 920 does not define the term "cost-effective." Dictionaries, in general, define "cost-effective" as the quality of being economical in terms of the benefits, including goods or services received for the money spent.[42] Interpreting "cost-effective" as requiring a precise measurement of effectiveness of a particular technology vis-à-vis its cost to an issuer as well as merchants would necessitate, in addition to an issuer calculating its own implementation costs, the extremely burdensome and complex analyses of calculating the costs to merchants and others of implementing and using the fraud-prevention technology and isolating the amount of fraudulent electronic debit transactions prevented by a particular technology, rather than by other means. Moreover, the complexity of this analysis would be increased further if an issuer were required to demonstrate cost-effectiveness prior to implementing a new technology or else take the risk of investing in a new technology only to find afterwards that it could not demonstrate the technology's cost-effectiveness and, thus, not be eligible to receive a fraud-prevention adjustment.

An alternate interpretation of the cost-effectiveness requirement is that, instead of requiring an issuer to affirmatively demonstrate the cost-effectiveness of a particular fraud-prevention technology, the requirement acts as a limitation on the fraud-prevention methods the Board's standards may require issuers to develop and implement. Thus, the Board could not adopt standards that would require an issuer to develop and implement new fraud-prevention technologies the costs of which far exceed any expected benefit from adopting the technologies.[43]

EFTA Section 920(a)(5)(A)(ii) is silent as to which party's perspective is relevant for the cost-effectiveness of a particular technology. EFTA Section 920(a)(5)(B) requires the Board to consider, among other factors, the fraud-prevention and data-security costs expended by each party involved in electronic debit transactions. There are numerous fraud-prevention methods an issuer may use or adopt. Some of these fraud-prevention methods, such as the use of neural networks, do not impose costs on other parties to the transaction. Other fraud-prevention methods, such as card-authentication technology built into the card, impose costs on merchants that must ensure their point-of-sale terminals are compatible with the card-authentication technology embedded in the card. Therefore, the Board believes that it is appropriate, when assessing the cost-effectiveness of a particular fraud-prevention technology, for an issuer to consider whether and to what extent the fraud-prevention method it implements will impose costs on other parties. The Board recognizes, however, that an issuer may not have complete information about the costs that other parties may incur. Nonetheless, an issuer should consider

[41] This commenter also suggested that the Board continue to gather information about the costs of new fraud-prevention activities.

[42] Merriam-Webster Dictionary, *available at* http://www.merriam-webster.com; American Heritage Dictionary, *available at* http://ahdictionary.com**.**

[43] As discussed above in connection with § 235.4(a), the Board has set the adjustment amount equal to the cost of the median issuer to give consideration to, and take into account, the fraud-prevention costs of other parties (as opposed to the interchange fee standards in § 253.3, which were set at the 80th percentile issuer) and to place additional cost discipline on issuers to ensure that their fraud-prevention activities are cost effective.

the approximate magnitude of the costs imposed on other parties, even though an issuer may not have complete information about the extent of the costs imposed on other parties.

New comment 4(b)-5 clarifies that a consideration of the cost-effectiveness of a fraud-prevention technology involves considering the expected cost of a technology relative to the expected effectiveness of that technology in reducing fraud. This approach recognizes that an issuer likely will be unable to measure the issuer's actual cost and the actual effectiveness of a fraud-prevention technology, particularly if the technology is new, but will be able to form a reasonable expectation as to both the cost of and effectiveness of a given fraud-prevention technology. In calculating the expected cost of a particular fraud-prevention method, an issuer should consider both the expected initial implementation costs and the expected ongoing costs of using the fraud-prevention method.

New comment 4(b)-6 provides that an issuer need not develop fraud-prevention technologies itself to satisfy the standards in § 235.4(b), but may implement appropriate fraud-prevention technologies developed by a third party. Fraud-prevention technologies vary in their technological complexity, including the technological expertise and investment required for their development. Issuers—typically entities engaged in banking activities—often do not have the technological expertise to develop, or have opted not to specialize in the development of, complex fraud-prevention technologies. Instead, issuers often purchase fraud-prevention solutions (e.g., neural networks) developed by third parties. Although not developed by the issuer, these technologies nonetheless may be cost effective. Moreover, many issuers would not find it to be economical to devote resources to in-house research and development of all the fraud-prevention technologies they implement.

III. § 235.4(b)(2) Required Elements of an Issuer's Policies and Procedures

Section 235.4(b)(1) of the interim final rule requires an issuer, in order to be eligible to charge or receive a fraud-prevention adjustment, to develop and implement policies and procedures reasonably designed to (i) identify and prevent fraudulent electronic debit transactions, (ii) monitor the incidence of, reimbursements received for, and losses incurred from fraudulent electronic debit transactions, (iii) 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 (iv) secure debit card and cardholder data. The interim final rule's commentary to § 235.4(b)(1) provides additional detail on the types of policies and procedures considered reasonably designed to achieve the fraud-prevention objectives in §§ 235.4(b)(1)(i) through (iv).

In addition to the comments received on the overall framework of the fraud-prevention standards (discussed above), the Board received more targeted comments on the policies and procedures designed to achieve the specified fraud-prevention objectives. These comments are discussed below in connection with each fraud-prevention objective.

In the final rule, revised § 235.4(b)(1) more generally requires an issuer to develop and implement policies and procedures that are "reasonably designed to take effective steps to reduce the occurrence of, and costs to all parties from, fraudulent electronic debit transactions." Section 235.4(b)(2), in turn, sets forth elements of a fraud-prevention program that an issuer's policies

and procedures must address. The Board believes, for the reasons set forth below, that developing and implementing policies and procedures that address these specific elements are steps that are effective in reducing the occurrence of, and costs from, fraudulent electronic debit transactions. These required aspects of a fraud-prevention program are similar to the fraud-prevention objectives in interim final rule § 235.4(b)(1).

Several commenters emphasized that one of the benefits of a non-prescriptive approach to fraud-prevention is that such an approach provides an issuer with greater flexibility to tailor its fraud-prevention program to the size and scope of its debit card program and to ever-changing fraud-types and patterns. The Board agrees that a flexible approach to fraud prevention is preferable to a one-size-fits-all approach. Accordingly, the Board has determined to add new comment 4(b)(2)-1 that provides that an issuer may tailor its fraud-prevention policies and procedures to address its particular debit card program. Relevant considerations when tailoring its policies and procedures include the size of its debit card program, the types of transactions in which its cardholders commonly engage (e.g., card-present or card-not-present), fraud types and methods experience by the issuer, and the cost of implementing new fraud-prevention methods in light of the expected reduction in fraud from implementing such new methods. Likewise, the Board recognizes that an issuer may determine that fraud-prevention factors other than those listed in §§ 235.4(b)(2)(i) – (iv) are appropriate for its policies and procedures to address. Accordingly, the Board has determined to revise § 235.4(b)(2) to provide that an issuer's policies and procedures also must address "such other factors as the issuer considers appropriate."

A. § 235.4(b)(2)(i) Identify and Prevent Fraudulent Transactions

In interim final rule § 235.4(b)(1), the first fraud-prevention objective of an issuer's policies and procedures is identifying and preventing fraudulent electronic debit transactions. The commentary to interim final rule § 235.4(b)(1) provides that an issuer's policies and procedures should include activities to prevent, detect, and mitigate fraud even if the costs of the activities are not recoverable as part of the fraud-prevention adjustment. The commentary also provides examples of policies and procedures designed to identify and prevent fraudulent electronic debit transactions. For example, an issuer could use an automated mechanism to assess the risk that a particular electronic debit transaction is fraudulent during the authorization process. An issuer also could implement practices that support cardholder-reporting of lost or stolen cards or suspected incidences of fraud. The commentary also provides that an issuer could specify the use of particular technologies or methods to better authenticate the cardholder at the point of sale. Finally, the commentary provides that an issuer's policies and procedures should include an assessment of the effectiveness of the different authentication methods that the issuer enables its cardholders to use and that, if the issuer determines one method is more effective than the other, the issuer should consider practices to encourage its cardholders to use the more effective authentication method, as well as consider adopting new methods of authentication that are materially more effective than those currently available to its cardholders.

One commenter suggested that Board state in the commentary that an issuer should review the effectiveness of its authorization rules that govern automated fraud-detection mechanisms. Another commenter suggested that the Board add language encouraging issuers to specify the use of particular technologies or methods in order to authenticate the payment device

and cardholder at the time of the transaction because there may be two authentication processes—one that identifies the card and one that identifies the cardholder.[44]

Section 235.4(b)(2)(i) of the final rule requires that an issuer's policies and procedures address "methods to identify and prevent fraudulent electronic debit transactions." The Board has revised comment 4(b)(2)(i)-1.i (interim final rule comment 4(b)(1)(i)-2.iii) to include the concept of card authentication at the time of the transaction, as suggested by the commenter, in recognition of the fact that fraud may be in the form of unauthorized use of a legitimate debit card or unauthorized use of a counterfeit debit card. The Board believes that an issuer should implement policies and procedures designed to prevent both types of fraud. The Board also has revised comment 4(b)(2)(i)-1.i to clarify that an issuer may specify the use of particular technologies or methods only to the extent that doing so does not inhibit the ability of a merchant to direct the routing of electronic debit transactions for processing over any payment card network that may process such transactions (*see* § 235.7 and commentary thereto). In other words, an issuer may not specify the use of a particular technology if that technology is enabled for only one network, or two affiliated networks, on the debit card, but may specify the use of a particular technology that is available for at least two unaffiliated networks enabled on the card. This addition prevents potential conflicts with Regulation II's other requirements.

In addition, the Board has adopted comments 4(b)(2)(i)-1.ii and 4(b)(2)(i)-1.iii as set forth in interim final rule comments 4(b)(1)(i)-1.i and 4(b)(1)(i)-1.ii, respectively, and has made minor clarifying changes to comment 4(b)(2)(i)-1.iii. The Board has not revised the commentary to provide that an issuer review the effectiveness of any rules for its automated fraud-detection mechanisms, as suggested by a commenter. This review is encompassed in new § 235.4(b)(3), which requires an issuer to review its policies and procedures, and their implementation, in light of their effectiveness.

B. § 235.4(b)(2)(ii) Monitoring the Volume and Value of its Fraudulent Transactions

Section 235.4(b)(1)(ii) of the interim final rule requires issuers to monitor the incidence of, reimbursements received for, and losses incurred from fraudulent electronic debit transactions. Under that section, an issuer's policies and procedures must be designed to monitor the types, number, and value of electronic debit transactions, as well as its and its cardholders' losses from fraudulent electronic debit transactions, fraud-related chargebacks to acquirers, and reimbursements from other parties (such as from fines assessed to merchants for noncompliance with Payment Card Industry Data Security Standards). (*See* interim final rule comment 4(b)(1)(ii)-1). The Board imposed this monitoring requirement on issuers as necessary in order for an issuer to inform its policies and procedures. The Board received one comment related to the monitoring requirement. This commenter expressed support for the standard's flexibility in requiring issuers to monitor the incidence of fraud. The final rule retains the requirements that the policies and procedures developed and implemented by an issuer address monitoring the

[44] The other comments the Board received on this provision and accompanying commentary focused primarily on the issuer's review of the authentication methods it makes available to its cardholders. As discussed above, the Board has moved the commentary paragraphs applicable to an issuer's review of its policies and procedures to the commentary to § 235.4(b)(1). Accordingly, these comments are discussed in connection with § 235.4(b)(1) and accompanying commentary.

volume and value of its fraudulent electronic debit transactions, as well as the types of fraudulent electronic debit transactions it experiences.

The Board has made minor, clarifying revisions to comment 4(b)(2)(ii)-1 (interim final rule comment 4(b)(1)(ii)-1). Specifically, the Board has revised this comment to clarify that the monitoring requirement is imposed on an issuer with respect to the number and value of the issuer's fraudulent electronic debit transactions, as opposed to the number and value of fraudulent transactions experienced across the industry. The Board also has revised comment 4(b)(2)(ii)-1 in recognition of the fact that an issuer may not be able to monitor the value of losses imposed on its cardholders by merchants. Rather, issuers must monitor the losses from fraudulent transactions that it passes on to its cardholders. Finally, the Board has revised comment 4(b)(2)(ii)-1 to emphasize that an issuer should establish procedures to retain fraud-related information necessary to perform its reviews under § 235.4(b)(3) and to retain and report information as required under § 235.8.

C. § 235.4(b)(2)(iii) Appropriate Response to Suspicious Transactions

Section 235.4(b)(1)(iii) of the interim final rule requires an issuer to develop and implement policies and procedures reasonably designed to "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." Interim final rule comment 4(b)(1)(iii)-1 explains that whether an issuer's response to fraudulent or suspicious electronic debit transactions is appropriate depends on the circumstances and the risk of future fraudulent electronic debit transactions. The comment also provides examples of appropriate responses. Interim final rule comment 4(b)(1)(iii)-2 clarifies 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.

The Board received comments on this provision from two issuers. One issuer supported the Board's position that an "appropriate" response depends on the circumstances and suggested that the Board clarify that these "circumstances" include an issuer's debit card program, specific fraud experiences, and data analysis. Another issuer expressed concern that comment 4(b)(1)(iii)-2 could be construed in a manner that adversely affects the incentives and risks imposed by network rules (e.g., the chargeback rules).

The final rule retains the requirement that an issuer's policies and procedures address appropriate responses to suspicious electronic debit transactions. The Board, however, has revised § 235.4(b)(2)(iii) (interim final rule § 235.4(b)(1)(iii)) to clarify that an issuer's response should be designed to limit potential costs to all parties from fraudulent electronic debit transactions. The Board has made changes to comment 4(b)(2)(iii)-1 (interim final rule comment § 235.4(b)(1)(iii)-1) to clarify that the issuer's assessment of the risk of future fraudulent electronic debit transactions is one example of the facts and circumstances that determines the appropriateness of the response.

Interim final rule comment 4(b)(1)(iii)-2 provides that merely shifting the loss to another party is not an appropriate response to a suspicious electronic debit transaction. One commenter

expressed concern that this statement could adversely affect network rules that allocate fraud losses. Interim final rule comment 4(b)(1)(iii)-2 was intended to emphasize that an issuer's response should mitigate the issuer's fraud losses in addition to the fraud losses of other parties. The Board, however, does not believe that interim final rule comment 4(b)(1)(iii)-2 is necessary to provide guidance on the appropriateness of an issuer's response to suspicious transactions in light of the clarifications to revised § 235.4(b)(2)(iii). Accordingly, the Board has removed the comment.

D. § 235.4(b)(1)(iv) Data Security

Section 235.4(b)(1)(iv) of the interim final rule requires an issuer to develop and implement policies and procedures reasonably designed to secure debit card and cardholder data. Interim final rule comment 4(b)(1)(iv) further explains that debit card and cardholder data should be secured during transaction processing, during storage by the issuer (or its service provider), and when carried on media by employees or agents of the issuer. That comment recognizes that this standard may be incorporated into an issuer's information security program required by Section 501(b) of the Gramm-Leach-Bliley Act.[45]

One commenter suggested that the Board revise its commentary to require an issuer to secure debit card and cardholder data only when such data are transmitted by the issuer and not apply the requirement to situations where the issuer is receiving data, because the issuer cannot control the transmission of data from third parties. As set forth in the interim final rule, comment 4(b)(1)(iv) states that an issuer should secure debit card and cardholder data when the issuer or its service provider is the party transmitting or storing the data. Although the issuer may not have direct control over every piece of information transmitted by its service provider, the issuer should select a service provider that sufficiently secures data the service provider transmits that relates to the issuer's debit cards and cardholders' data. An issuer is not required to develop and implement policies and procedures that address the security of debit card and cardholder information when received and processed by third parties that are not acting as the issuer's agent. Accordingly, the Board has determined not to make any changes to § 235.4(b)(2)(iv) (interim final rule § 235.4(b)(1)(iv)) and the accompanying commentary as set forth in the interim final rule.

IV. Section 235.4(b)(3) Review of Policies and Procedures

Section 235.4(b)(2) of the interim final rule requires an issuer to review its fraud-prevention policies and procedures at least annually and to update those policies and procedures as necessary to address changes in the prevalence and nature of fraudulent electronic debit transactions and available methods of detecting, preventing, and mitigating fraud. Interim final rule comment 4(b)(2) explains that an issuer may need to review and update its policies and procedures more frequently than once a year; an additional review could be necessary, for example, if there is a significant change in fraud types, fraud patterns, or fraud-prevention methods or technologies before an issuer's next-scheduled annual review. In addition, comment 4(b)(1)(i)-2 to the interim final rule provides that an issuer should assess of the effectiveness of the different authentication methods that the issuer enables its cardholders to use and that, if the

[45] *See* 15 U.S.C. 6805.

issuer determines one method is more effective than the other, the issuer should consider practices to encourage its cardholders to use the more effective authentication method, as well as consider adopting new methods of authentication that are materially more effective than those currently available to its cardholders.

The Board received comments on both of these provisions related to an issuer's review of its policies and procedures. One issuer explicitly supported requiring issuers to review their fraud-prevention policies and procedures on an annual basis. This issuer also suggested that, rather than requiring additional reviews based on the undefined "significant change" in fraud or fraud patterns, an issuer should determine whether changes in fraud types, fraud patterns, or fraud-prevention technologies or methodologies have an impact on the issuer's policies and procedures that would require additional review of and update to its policies and procedures.

One issuer suggested that the Board revise the language in comment 4(b)(1)(i)-2 to the interim final rule to recognize that the effectiveness of an authentication method in preventing fraud is only one of many factors issuers consider in promoting a particular authentication method, and that other factors an issuer may consider include acceptance and cost. In addition, one issuer argued that whether a particular authentication method is "materially more effective" should be determined by each issuer and that issuers should not be required to adopt any specific authentication method.[46] By contrast, merchant commenters supported standards that would require issuers to promote the technology with the lowest rate of fraud, as opposed to requiring that an issuer "consider" promoting the lower-fraud technology.

Section 235.4(b)(3) of the final rule retains the requirement that an issuer review, at least annually, its fraud-prevention policies and procedures, and their implementation, and update them as necessary. The Board, however, has revised the review requirement to provide more guidance on the required elements of the reviews and when reviews and updates to an issuer's policies and procedures, and their implementation, are necessary.

Section 235.4(b)(3)'s review requirement is intended to ensure that an issuer continues to take effective steps to reduce fraudulent electronic debit transactions, including through the development and implementation of cost-effective technologies. Accordingly, the Board has revised the provision relating to an issuer's review to require an issuer to review its policies and procedures, and their implementation, in light of their effectiveness (§ 235.4(b)(3)(i)) and cost-effectiveness (§ 235.4(b)(3)(ii)). New comment 4(b)(3)-1.i provides that an issuer's assessment should consider whether its policies and procedures are reasonably designed to reduce the number and value of its fraudulent electronic debit transactions relative to its non-fraudulent electronic debit transactions and are cost effective.[47]

The Board has made additional revisions to the interim final rule's requirement that an issuer update its policies and procedures, as necessary, "to address changes in the prevalence and nature of fraudulent electronic debit transactions and available methods of detecting, preventing,

[46] Some issuers recommended that the Board provide more detail regarding the meaning of the phrase "materially more effective." In light of the revisions to § 235.4(b)(1) and accompanying commentary, it is unnecessary to address those comments.

[47] Comments 4(b)(1)-2 through 4(b)(1)-6 provide additional guidance on effectiveness and cost-effectiveness.

and mitigating fraud." One reason for adopting the non-prescriptive approach to fraud-prevention standards is to ensure that an issuer has sufficient flexibility to adjust its fraud-prevention methods in light of the rapidly changing nature of fraud and the availability of fraud-prevention methods. For this flexibility to be most beneficial and effective in preventing fraudulent electronic debit transactions, an issuer must update its policies and procedures in light of the changing nature of fraud and availability of fraud-prevention methods. The Board, however, believes that the most important source of information to an issuer about types and methods of fraud is the issuer's own experience and information. The Board also believes the additional burden on issuers of continuous open-ended monitoring of the types of fraud and methods used to commit fraud throughout the industry may exceed the benefit of this information to the issuers. To the extent an issuer experiences changes in fraud types and methods, it should identify them through its monitoring and update its policies and procedures, as necessary, in light of the subsequent identification from its own experience.

In addition to its own experience, an issuer may learn of changes in the types of fraud, methods used to commit fraud, and available methods for detecting and preventing fraud from other sources. Specifically, payment card networks may provide their issuers with information regarding common types and methods of fraudulent transactions based on the networks' monitoring of transactions or may provide an issuer with information on new fraud-prevention methods that are available for an issuer to enable on its cards. In addition, law enforcement agencies or fraud-monitoring groups in which the issuer participates may inform the issuer of changes in the nature of fraud and available methods of preventing fraud. Finally, an issuer may learn of changes in the nature of fraud and fraud-prevention methods from supervisory guidance. The Board believes that, at a minimum, an issuer should be expected to consider any changes in the types of fraud, methods used to commit fraud, and available methods to prevent fraudulent electronic debit transactions that it learns about from these sources. The Board, therefore, has revised § 235.4(b)(3) to specify the sources of information regarding the changing nature of fraud and available methods of preventing fraud that an issuer must consider in determining whether updates to its policies and procedures are necessary.

New comment 4(b)(3)-2 provides that an issuer may need to review its policies and procedures more frequently than on an annual basis based on information obtained from monitoring its fraudulent electronic debit transactions, changes in the types or methods of fraud, and available fraud-prevention methods. The revised comment eliminates the "significant change" trigger in the interim final rule and requires an issuer to determine whether more frequent review is necessary. The Board considered the comments received on this provision and determined that objectively defining "significant change" could inhibit an issuer from more frequently reviewing its policies and procedures. Each issuer will have unique fraud-prevention programs, and a change in debit card fraud, industry fraud types and methods, and available fraud-prevention methods may be "significant" for one issuer, but not another issuer. Therefore, the Board believes that an issuer will be in the best position to determine whether changes in its debit card fraud, industry trends in fraud types and methods, and available fraud-prevention methods necessitate a more-frequent-than-annual review of its fraud-prevention programs. An issuer's determination as to the necessity of more frequent reviews and updates is subject to supervisory review under § 235.9.

The Board has added new comment 4(b)(3)-3 to provide guidance on the interaction between an issuer's required fraud-prevention program reviews and updates and an issuer's eligibility to receive the fraud-prevention adjustment under § 235.4. The required review of an issuer's fraud-prevention policies and procedures, and their implementation, is intended to ensure that an issuer's policies and procedures continue to be reasonably designed to take effective steps to reduce the occurrence of, and costs to all parties from, fraudulent electronic debit transactions. The review requirements also ensure that an issuer is assessing its fraud-prevention policies and procedures against changing fraud trends and available fraud-prevention methods. The Board anticipates that updates to an issuer's fraud-prevention policies and procedures may be necessary, although the Board does not expect substantial updates to be necessary often.

An issuer could be deterred from making necessary updates to its policies and procedures if an issuer becomes ineligible to receive the fraud-prevention adjustment after merely determining that any updates to its fraud-prevention program are necessary. In fact, one of the effective steps that an issuer can take to prevent fraudulent electronic debit transactions, and reduce the losses from such transactions, is to revise its fraud-prevention policies and procedures to make them more effective. Therefore, the Board has added new comment 4(b)(3)-3 to provide that an issuer does not become ineligible to receive the fraud-prevention adjustment merely because it determines updates are necessary or appropriate. In order to remain eligible to receive or charge a fraud-prevention adjustment under § 235.4, however, an issuer should develop and implement such updates as soon as reasonably practicable in light of the circumstances. For example, an issuer may determine that it should enable new card-authentication methods, and such new card-authentication methods require the reissuance of cards. Such an issuer should issue the new cards as soon as reasonably practicable in light of the process for ordering new cards and distributing them to cardholders. This process could take longer than, for example, improving algorithms on a neural network program it uses.

V. Section 235.4(c) Notification

Section 235.4(c) of the interim final rule provides that, in order to be eligible to receive or charge a fraud-prevention adjustment, an issuer that satisfies the standards set forth in § 235.4(b) must certify its compliance to its payment card networks on an annual basis. The interim final rule does not establish a process for this certification and, instead, leaves it up to the payment card networks to develop their own processes for identifying issuers eligible for the adjustment. Interim final rule comment 4(c)-1.

The Board received several comments on the certification provision. Merchants and their trade groups generally opposed the certification provision because they believed that the issuers and networks would be the ultimate judges of whether an issuer's policies and procedures satisfy the Board's standards. One commenter expressed concern that placing the compliance determination with the network would lead each network to favor its own fraud-prevention technology. Commenters that opposed placing the compliance determination with issuers and networks suggested that, alternatively, issuers should be required to certify their compliance with the fraud-prevention standards to their regulator in order to ensure that issuers are receiving adjustments only when the issuer complies with the Board's standards. One commenter

supported a network-certification requirement but only if such a requirement was limited to identifying which issuers have self-certified as complying with the Board's standards.

The Board also received comments on whether the Board should establish a uniform certification process, assuming the Board required some certification. Some issuers opposed establishing a uniform certification process in support of allowing industry participants to develop the process. These issuers argued that industry-established processes would enable more consistency with the network-established processes for identifying issuers that are exempt and not exempt from the interchange fee standard. One commenter thought a network-established process was appropriate because networks currently are able to ensure compliance with the network's fraud-prevention standards. By contrast, other commenters representing issuers supported the Board establishing a consistent certification process across networks to ensure that all issuers are treated fairly, provided that the process is sufficiently flexible to support operational and system differences across networks. Other commenters recommended that the Board establish a uniform certification process that would allow consumers and merchants to have access to compliance filings.

The final rule requires an issuer to inform its payment card networks, on an annual basis, of its compliance with the rule's fraud-prevention standards in § 235.4(b) before the issuer may receive or charge a fraud-prevention adjustment. The Board has, however, revised § 235.4(c) to refer to this requirement as a "notification" requirement instead of a "certification" requirement, as in the interim final rule. Based on the comments received, the term "certification" connoted a more official and final determination by the issuer and payment card networks of an issuer's compliance than the Board intended. Compliance with the fraud-prevention standards in § 235.4(b), like compliance with all other provisions of Regulation II, is subject to administrative enforcement in accordance with § 235.9. Accordingly, the Federal agency with responsibility for enforcing an issuer's compliance with Regulation II is the entity that ultimately determines an issuer's compliance with the Board's fraud-prevention standards. The Board believes that referring to the requirement as a "notification" more accurately conveys that the purpose of this requirement is to place an affirmative requirement on an issuer to inform networks of what the issuer has determined to be its compliance with the fraud-prevention standards.

The Board also did not establish a uniform notification process in its final rule. In issuing the final rule implementing the other provisions of EFTA Section 920, the Board determined not to establish a uniform certification process for issuers that were exempt from the interchange fee standards or that issued debit cards that were exempt from the interchange fee standards.[48] The Board continues to believe that payment card networks should have the flexibility to develop their own processes for identifying issuers that are eligible to receive a fraud-prevention adjustment.[49] The Board believes it is unnecessary to impose additional processes by rule that serve the same function as those already developed by payment card networks. The final rule,

[48] 76 FR 43394, 43437 – 38 (Jul. 20, 2011).

[49] This flexibility is similar to that which payment card networks have in establishing processes to determine the status of issuers that do not appear on the Board's list of exempt institutions with consolidated assets below $10 billion, issuers of debit cards issued pursuant to government-administered payment programs, and issuers of certain reloadable, general-use prepaid cards.

however, continues to specify that an issuer must notify its payment card networks of its compliance on an annual basis.

VI. Section 235.4(d) Change in Status

The interim final rule does not explicitly address steps an issuer must take if it is found to be non-compliant with the Board's fraud-prevention standards by the Federal agency with responsibility for enforcing compliance with Regulation II. One network encouraged the Board to provide for a cure period in the event the Federal agency with responsibility to enforce an issuer's compliance under § 235.9 determined that a particular issuer was no longer eligible to receive a fraud-prevention adjustment. This network suggested that the Board allow such an issuer 90 to 180 days to come into compliance after a finding of a deficiency. This network also supported providing networks 30 days advance notice prior to the date on which an issuer may no longer receive a fraud-prevention adjustment in order to allow the network to reprogram its systems.

The Board has added new § 235.4(d) to the final rule to address a change in the issuer's compliance status. EFTA Section 920(a)(5) provides that the Board may allow for a fraud-prevention adjustment to the permissible interchange fee only if an issuer complies with the Board's fraud-prevention standards. As recognized in new comment 4(b)(3)-3, in the course of reviewing its fraud-prevention policies and procedures, an issuer may determine that updates are necessary. Likewise, the agency with responsibility for enforcing an issuer's compliance with Regulation II under § 235.9 also may identify updates that are necessary for an issuer to continue to be eligible to receive or charge a fraud-prevention adjustment. Merely determining that updates to its policies and procedures are necessary does not render an issuer ineligible to receive or charge a fraud-prevention adjustment; the Board anticipates that issuers may need to update their policies and procedures regularly to ensure their continued effectiveness and cost-effectiveness.

The Board believes that if an issuer is in substantial non-compliance with the Board's fraud-prevention policies and procedures, the issuer should not be eligible to receive a fraud-prevention adjustment. Under the non-prescriptive approach adopted by the Board, there are likely to be varying degrees of deficiencies in an issuer's fraud-prevention policies and procedures. Whether the deficiencies constitute substantial non-compliance will depend on the facts and circumstances, including the severity of the deficiencies. For example, an issuer's policies and procedures may fail to address appropriate responses to suspicious transactions as required by §235.4(b)(2)(iii). Another issuer's policies and procedures may address appropriate responses to suspicious transactions, but the manner in which the response is made may be less effective in light of recent changes to fraud types experienced by the issuer. Failure to address an entire category of fraud-prevention activity could be one circumstance in which an issuer is substantially non-compliant with the Board's fraud-prevention standards.

New § 235.4(d) provides that an issuer is not eligible to receive or charge a fraud-prevention adjustment if the issuer is substantially noncompliant with the Board's fraud-prevention standards in § 235.4(b). A finding of substantial noncompliance would be made by the issuer or the Federal agency with responsibility for enforcing an issuer's compliance with Regulation II under § 235.9. New § 235.4(d) also provides that an issuer found to be

substantially noncompliant with the Board's standards must notify its payment card networks that it is no longer eligible to receive or charge a fraud-prevention adjustment no later than 10 days after determining or receiving notification from the appropriate agency under § 235.9 that the issuer is substantially noncompliant. In addition, the issuer must stop receiving and charging the fraud-prevention adjustment no later than 30 days after notifying its payment card networks. This is the amount of time that a network-commenter suggested as the minimum amount of time necessary for a network to reprogram its interchange fee schedules. The Board does not believe it is necessary to incorporate a cure period in the final rule because the need to regularly update an issuer's policies and procedures does not make the issuer ineligible to receive the fraud-prevention adjustment, assuming the updates are made on a timely basis. Moreover, the Board does not believe that issuers in substantial noncompliance with the Board's standards should be entitled to receive the fraud-prevention adjustment during a cure period.

In addition, the final rule does not specify the steps an issuer must take to become eligible to receive the fraud-prevention adjustment after it has come into compliance. A determination of substantial non-compliance will be made by the appropriate agency under § 235.9. The Board believes that it is appropriate for that agency to determine the steps an issuer must take to satisfy the agency that the issuer has remedied deficiencies in its fraud-prevention program.

EFTA 904(a) Economic Analysis

I. Statutory Requirement

Section 904(a)(2) of the EFTA requires the Board to prepare an economic analysis of the impact of the regulation that considers the costs and benefits to financial institutions, consumers, and other users of electronic fund transfers. The analysis must address the extent to which additional paperwork would be required, the effect upon competition in the provision of electronic fund transfer services among large and small financial institutions, and the availability of such services to different classes of consumers, particularly low income consumers.[50]

II. Cost/Benefit Analysis

The **Section-by-Section Analysis** above, as well as the **Final Regulatory Flexibility Analysis** and **Paperwork Reduction Act** analysis below, contain a more detailed discussion of the costs and benefits of various aspects of the proposal. This discussion is incorporated by reference in this section.

As permitted by Section 920(a)(5) of the EFTA, this final rule allows an issuer that is subject to the interchange fee standards to receive or charge an amount of no more than 1 cent per transaction in addition to its interchange transaction fee if the issuer develops and implements policies and procedures that are reasonably designed to take effective steps to reduce the occurrence of, and costs to all parties from, fraudulent electronic debit transactions.[51] The

[50] This analysis considers the competition between "covered issuers" (i.e., those that, together with affiliates, have assets of $10 billion or more) and "exempt issuers" (i.e., those that, together with affiliates, have assets of less than $10 billion).

[51] The interchange fee standards provide that an issuer may not receive or charge an interchange transaction fee in excess of the sum of a 21-cent base component and 5 basis points of the transaction's value. Certain issuers and

final rules sets forth fraud-prevention aspects that an issuer's policies and procedures must address and requires an issuer to review its policies and procedures at least annually, and update them as necessary in light of their effectiveness, cost-effectiveness, and changes in the types of fraud, methods used to commit fraud, and available fraud-prevention methods. An issuer must notify its payment card networks annually that it complies with the Board's fraud-prevention standards and must also notify its payment card networks that it is no longer eligible to receive or charge a fraud-prevention adjustment no later than 10 days of determining or receiving notification from the appropriate agency under § 235.9 that the issuer is substantially non-compliant with the Board's fraud-prevention standards. The issuer must stop receiving or charging the fraud-prevention adjustment no later than 30 days after notifying its networks.

A. Additional Paperwork

The collection of information required by this final rule is found in § 235.4 of Regulation II (12 CFR part 235). The new paperwork requirements of this final rule are discussed below in the **Paperwork Reduction Act** section, which contains a more detailed estimate for burden hours for being eligible to receive or charge the fraud-prevention adjustment. This final rule does not impose additional paperwork requirements related to the reporting to the Board required under § 235.8; issuers that do not qualify for the small issuer exemption ("covered issuers") would be required to provide cost data to the Board independent of whether they qualify for the fraud-prevention adjustment. Covered issuers also would be required under § 235.8 to retain records that demonstrate compliance with the requirements of Regulation II for not less than five years after the end of the calendar year in which the electronic debit transaction occurred. If an issuer receives actual notice that it is subject to an investigation by an enforcement agency, the issuer must retain the records until final disposition of the matter. For smaller institutions that are not required to submit cost information to the Board under Regulation II, the regulation does not impose any reporting requirements.

B. Competition in the Provision of Services Among Financial Institutions

As required by EFTA Section 920(a)(6), Regulation II exempts small issuers (i.e., those issuers that, together with affiliates, have consolidated assets of less than $10 billion) from the interchange fee standards, as well as the provisions relating to the fraud-prevention standards and adjustment. Regulation II, however, does not mandate that payment card networks adopt a two-tier interchange fee structure in which exempt issuers receive higher interchange fees. Since the interchange fee provisions of Regulation II (including the 1-cent fraud-prevention adjustment) became effective on October 1, 2011, most payment card networks have offered a two-tier interchange fee structure in which exempt issuers receive higher average interchange fees than those received by non-exempt issuers.[52] The 1-cent adjustment in the final rule, which is already

products are exempt from the interchange fee restrictions, including small issuers that, together with their affiliates, have less than $10 billion in assets; certain cards accessing government-administered payment programs; and certain reloadable general-use prepaid cards that are not marketed or labeled as a gift certificate or gift card. Payment card networks may, but are not required to, differentiate between interchange fees received by covered issuers and products versus exempt issuers and products.

[52] See http://www.federalreserve.gov/paymentsystems/regii-average-interchange-fee.htm.

permitted under the interim final rule, is not likely to affect the continuation of a two-tier interchange fee structure.[53]

Some covered issuers may find that the additional cost of complying with the fraud-prevention standards are greater than the additional revenue generated from receiving the adjustment and so choose to not qualify for the adjustment. To the extent payment card networks provide the adjustment, covered issuers that qualify for the adjustment will likely experience an increase in their interchange revenue compared to covered issuers that do not qualify for the adjustment. In such a situation, covered issuers that do not qualify for the adjustment may need to adjust fees and account terms in response to the lower interchange revenue, whereas covered issuers that qualify may not. Under this scenario, consumers may shift their purchases of some financial services from covered issuers that do not qualify for the adjustment to exempt issuers or covered issuers that qualify for the adjustment in response to changes in fees and account terms at covered issuers that do not qualify for the adjustment. However, covered issuers that do not qualify for the adjustment and that have diversified product lines may look to retain customers by promoting alternative products not covered by the interchange fee standards, such as credit cards.

The competitive effects of any changes in fees or account terms across covered and exempt issuers due to the adjustment will depend on the degree of substitution among exempt issuers, covered issuers that qualify for the adjustment, and covered issuers that do not qualify for the adjustment. If the degree of substitutability of debit card and account services between covered issuers that qualify for the adjustment and covered issuers that do not qualify is large, then substantial shifts in the customer market share of each group of issuer may occur in response to less favorable changes in fees and account terms by issuers which do not qualify for the adjustment. Conversely, if substitution between covered issuers that qualify for the adjustment and covered issuers that do not is low, then any changes in fees and account terms may generate small shifts in customer market shares across covered issuers.

As the previous analysis suggests, the effect on competition among covered and exempt financial institutions will depend on a number of factors, including the extent to which payment card networks retain two-tier fee structures, the differentials in interchange fees across tiers in such structures, the product and service lines offered by covered and exempt financial institutions, and the substitutability of products and services across covered and exempt financial institutions. As noted above, most debit card networks have implemented two-tier fee structures. There is, however, no requirement that the networks continue to do so, and the level of interchange fees that will prevail in the long term is not known and will depend on market dynamics. Prior economic research suggests that competition between large and small depository institutions is weaker than competition within either group of institutions, likely because these institutions serve different customer bases.[54] For example, large institutions have

[53] See 76 FR 43394, 43463-64 for an analysis of the provision of two-tier interchange fee structure on the competition in the provision of services among financial institutions.

[54] *See, e.g.*, Robert Adams, Kenneth Brevoort, and Elizabeth Kiser, "Who Competes with Whom? The Case of Depository Institutions," *Journal of Industrial Economics*, March 2007, v. 55, iss.1, pp. 141-67; Andrew M. Cohen and Michael J Mazzeo, "Market Structure and Competition among Retail Depository Institutions," *Review of Economics and Statistics*, February 2007, v. 89, iss. 1, pp. 60-74; and Timothy H. Hannan and Robin A. Prager,

tended to attract customers who desire expansive branch and ATM networks and a wide variety of financial instruments. By contrast, smaller institutions often market themselves as offering more individualized, relationship-based service and customer support to consumers and small businesses. This research suggests that substitution effects in response to changes in fees or account terms are stronger between depository institutions of similar sizes than across depository institutions of different sizes. Therefore, there may be greater substitution away from covered issuers that do not qualify for the adjustment to covered issuers that do qualify for the adjustment because most covered issuers are large, but less substitution away from covered issuers that do not qualify to exempt issuers (which are mostly small).

III. Availability of Services to Different Classes of Consumers

The ultimate effect of the final rule on consumers will depend on the behavior of various participants in the debit card market. Specifically, the effect of the rule on any individual consumer will depend on a variety of factors, including the consumer's current payment behavior (e.g., cash user or debit card user), changes in the consumer's payment behavior, the competitiveness of the merchants from which the consumer makes purchases, changes in merchant payment method acceptance, and changes in the behavior of banks.

For low-income consumers, to the extent that fees and other account terms become more attractive as a result of the issuer receiving the adjustment, some low-income consumers may be more willing or more able to obtain debit cards and related deposit accounts. Similarly, more attractive fees and account terms may cause certain low-income consumers who previously did not hold debit cards and deposit accounts to use those products. At the same time, however, low-income consumers who currently use cash for purchases may face higher prices at the point of sale if retailers that they frequent set higher prices to reflect higher costs of debit card transactions because of the adjustment. Therefore, the net effect on low-income consumers will depend on various factors, including each consumer's payment and purchase behavior, as well as market responses to the rule.

IV. Conclusion

EFTA Section 904(a)(3) provides that "to the extent practicable, the Board shall demonstrate that the consumer protections of the proposed regulations outweigh the compliance costs imposed upon consumers and financial institutions." Based on the analysis above and in the **Section-by-Section Analysis**, the Board cannot, at this time, determine whether the benefits to consumers exceed the possible costs to financial institutions. The overall effects of the final rule on financial institutions and on consumers are dependent on a variety of factors, and the Board cannot predict the market response to the final rule.

Final Regulatory Flexibility Analysis

A final regulatory flexibility analysis (RFA) was included in the interim final rule in accordance with Section 3(a) of the Regulatory Flexibility Act, 5 U.S.C. 601 *et. seq.* (RFA). The Board incorporated by reference the final RFA analysis published with the other provisions of

---

"The Profitability of Small Single-Market Banks in an Era of Multi-market Banking," *Journal of Banking and Finance*, February 2009, v. 33, iss. 2, pp. 263-71.

the Board's Regulation II. The final analysis applicable to the other provisions of Regulation II applied to the regulation as a whole, including the fraud-prevention adjustment adopted in the interim final rule.

The RFA requires an agency to prepare a final regulatory flexibility analysis (FRFA) unless the agency certifies that the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities. The Board believes it is possible, but unlikely, that the fraud-prevention provisions in Regulation II will have a direct, significant economic impact on a substantial number of small entities.[55] Nonetheless, the Board has prepared the following FRFA pursuant to the RFA.

1. *Statement of the need for, and objectives of, the final rule*. EFTA Section 920 requires the Board to establish standards for assessing whether an interchange transaction fee received or charged by an issuer is reasonable and proportional to the cost incurred by the issuer with respect to the transaction. EFTA Section 920 authorizes the Board to allow for an adjustment to the amount of an interchange transaction fee received or charged by an issuer if (1) such adjustment is reasonably necessary to make an allowance for costs incurred by the issuer in preventing fraud in relation to electronic debit transactions involving that issuer, and (2) the issuer complies with fraud-prevention standards established by the Board. The final rule is intended to provide issuers with additional incentives to engage in activities that prevent fraud in relation to electronic debit transactions, and require issuers wishing to receive the adjustment to develop and implement fraud-prevention policies and procedures.

2. *Summary of significant issues raised by public comments in response to the Board's IRFA, the Board's assessment of such issues, and a statement of any changes made as a result of such comments*. The Board did not receive any comments explicitly about the final RFA included in the interim final rule. Commenters, however, discussed the proposed rule's impact on small entities, particularly small issuers. EFTA Section 920(a)(6)(A) and § 235.5(a) exempt from the interchange fee restrictions any issuer that, together with its affiliates, has assets of less than $10 billion. Consequently, like Regulation II's other provisions governing interchange fees, the provisions related to the fraud-prevention adjustment to the interchange fee restrictions do not directly affect small issuers. Commenters, however, were concerned that the small issuer exemption would not be effective in practice if payment card networks do not implement two-tier fee structures.

As mentioned above and in the preamble to the Board's final rule implementing the other provisions of EFTA Section 920, the Board is monitoring the effectiveness of the exemption for small issuers. The Board also publishes annual lists of institutions above and below the small issuer exemption asset threshold in order to reduce the administrative burden associated with identifying small issuers that qualify for the exemption. Based on information reported to the Board by payment card networks, the average interchange fee received by exempt issuers in the

[55] In addition, the final rule could have an indirect impact on small merchants due to the increased interchange fee small merchants may pay as a result of some covered issuers receiving or charging the 1-cent fraud-prevention adjustment. The size of this indirect impact, however, is difficult to predict and will depend on the number of debit card transactions performed by small merchants that are subject to the interchange fee standards, the pricing structures that acquirers offer to small merchants, and the fraud-prevention methods adopted by issuers.

fourth quarter of 2011, following the implementation of the interchange fee standard, was about the same as the amount they received in 2009.

3. *Description and estimate of small entities affected by the final rule*. This final rule applies directly to financial institutions that, together with affiliates, have assets of $10 billion or more. A financial institution generally is considered small if it has assets of $175 million or less.[56] Therefore, this final rule does not directly affect small entities.

4. *Projected reporting, recordkeeping, and other compliance requirements.* The Board's final rule does not apply to small entities and, therefore, in general, does not impose compliance requirements on small entities.[57]

5. *Steps taken to minimize the economic impact on small entities; significant alternatives*. In its proposed rule, the Board requested comment on any approaches, other than the proposed alternatives, that would reduce the burden on all entities, including small entities. As noted above, the Board will publish lists of institutions above and below the small issuer exemption asset threshold to facilitate the implementation of two-tier interchange fee structures (including the fraud-prevention adjustment) by payment card networks. In addition, the Board plans to publish annually information regarding the average interchange fees received by exempt issuers and covered issuers in each payment card network; this information may assist exempt issuers in determining the networks in which they wish to participate.

Paperwork Reduction Act

In accordance with the Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3501 - 3521; 5 CFR 1320 Appendix A.1), the Board has reviewed the final rule under the authority delegated to the Board by the Office of Management and Budget (OMB). The Board may not conduct or sponsor, and a respondent is not required to respond to, an information collection unless it displays a currently valid OMB control number. The OMB control number will be assigned.

On July 20, 2011, notice of the interim final rule was published in the *Federal Register* (76 FR 43478). The Board invited comment on (1) whether the proposed collection of information is necessary for the proper performance of the Board's functions, including whether the information has practical utility; (2) the accuracy of the Board's estimate of the burden of the proposed information collection, including the cost of compliance; (3) ways to enhance the quality, utility, and clarity of the information to be collected; and (4) ways to minimize the burden of information collection on respondents, including through the use of automated collection techniques or other forms of information technology. The comment period for the interim final rule expired on September 30, 2011. No comments were received specifically addressing the paperwork burden estimates. One commenter, however, stated that it was difficult to determine whether the Board's estimate of 40 hours to review an issuer's policies and procedures was adequate in light of the fact that the compliance burden could increase in the

[56] U.S. Small Business Administration, Table of Small Business Size Standards Matched to North American Industry Classification System Codes, available at http://www.sba.gov/idc/groups/public/documents/sba_homepage/serv_sstd_tablepdf.pdf.

[57] There may be some small financial institutions that have very large affiliates such that the institution does not qualify for the small issuer exemption.

future should the standards become more specific. The Board is restating its burden estimates from the interim final rule to reflect updates to the respondent count and to include burden estimates for the disclosure requirement under § 235.4(d), change in status.

The final rule contains requirements subject to the PRA. The collection of information required by this final rule is found in § 235.4 of Regulation II (12 CFR part 235). Under the final rule, if an issuer meets standards set forth by the Board, it may receive or charge an adjustment of no more than 1 cent per transaction to any interchange transaction fee it receives or charges in accordance with § 235.3.

To be eligible to receive the fraud-prevention adjustment under § 235.4(a)(1), an issuer must develop and implement policies and procedures reasonably designed to take effective steps to reduce the occurrence of, and costs to all parties from, fraudulent electronic debit transactions, including through the development and implementation of cost-effective fraud-prevention technology. An issuer's policies and procedures must address (1) methods to identify and prevent fraudulent electronic debit transactions; (2) monitoring of the volume and value of its fraudulent electronic debit transactions; (3) appropriate responses to suspicious electronic debit transactions in a manner designed to limit the costs to all parties from and prevent the occurrence of future fraudulent electronic debit transactions; (4) methods to secure debit card and cardholder data; and (5) such other factors as the issuer considers appropriate.

An issuer must review its fraud-prevention policies and procedures, and their implementation, at least annually, and update them as necessary in light of (i) their effectiveness in reducing the occurrence of, and cost to all parties from, fraudulent electronic debit transactions involving the issuer; (ii) their cost-effectiveness; and (iii) changes in the types of fraud, methods used to commit fraud, and available methods of detecting and preventing fraudulent electronic debit transactions that the issuer identifies from (A) its own experience or information; (B) information provided to the issuer by its payment card networks, law enforcement agencies, and fraud-monitoring groups in which the issuer participates; and (C) applicable supervisory guidance. Finally, an issuer must notify the payment card networks in which the issuer participates, on an annual basis, of its compliance with the Board's standards, as well as of its substantial noncompliance, as determined by the issuer or Federal agency with responsibility for enforcing the issuer's compliance with Regulation II. The final rule will be effective on October 1, 2012.

The final rule will apply to issuers that, together with their affiliates, have consolidated assets of $10 billion or more. The Board estimates that there are as many as 564 chartered issuers required to comply with the recordkeeping and reporting provisions under § 235.4.[58]

The Board estimates that the 564 issuers will take, on average, 160 hours (one month) to develop and implement policies and train appropriate staff to comply with the recordkeeping provisions under § 235.4. This one-time annual PRA burden is estimated to be 90,240 hours.

[58] For purposes of the PRA, the Board is estimating the burden for entities currently regulated by the Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, and National Credit Union Administration (collectively, the ''Federal financial regulatory agencies''). Such entities may include, among others, State member banks, national banks, insured nonmember banks, savings associations, and Federally-chartered credit unions.

On a continuing basis, the Board estimates issuers will take, on average, 40 hours (one business week) annually to review its fraud prevention policies and procedures, updating them as necessary, and estimates the annual PRA burden to be 22,560 hours. The Board estimates 564 issuers will take, on average, 30 minutes to comply with the disclosure provision under § 235.4(c) (annual notification), and estimates the annual reporting burden to be 282 hours. Lastly, the Board estimates 564 issuers will take, on average, 30 minutes to comply with the disclosure requirement under § 235.4(d) (change in status), and estimates the annual reporting burden to be 283 hours. The total annual PRA burden for this information collection is estimated to be 113,364 hours.

The Federal Reserve has a continuing interest in the public's opinions of our collections of information. At any time, comments regarding the burden estimate, or any other aspect of this collection of information, including suggestions for reducing the burden, may be sent to: Secretary, Board of Governors of the Federal Reserve System, Washington, DC 20551 Paperwork Reduction Project (Docket # R-1404), Washington, DC 20503.

Use of "Plain Language"

Section 722 of the Gramm-Leach-Bliley Act of 1999 (12 U.S.C. 4809) requires the Board to use "plain language" in all final rules published after January 1, 2000. The Board has sought to present this final rule in a simple and straight forward manner. The Board received no comments on whether the interim final rule was clearly stated and effectively organized, or on how the Board might make the text of the rule easier to understand.

Text of Final Rule

List of Subjects in 12 CFR Part 235

Banks, banking, Debit card routing, Electronic debit transactions, and Interchange transaction fees.

Authority and Issuance

For the reasons set forth in the preamble, the Board amends Title 12, Chapter II of the Code of Federal Regulations by revising § 235.4 to read as follows:

§ 235.4 Fraud–prevention adjustment

(a) *In general*. Subject to paragraph (b) of this section, an issuer may receive or charge an amount of no more than 1 cent per transaction in addition to any interchange transaction fee it receives or charges in accordance with § 235.3.

(b) *Issuer standards*. (1) To be eligible to receive or charge the fraud-prevention adjustment in paragraph (a), an issuer must develop and implement policies and procedures reasonably designed to take effective steps to reduce the occurrence of, and costs to all parties from, fraudulent electronic debit transactions, including through the development and implementation of cost-effective fraud-prevention technology.

(2) An issuer's policies and procedures must address—

(i) Methods to identify and prevent fraudulent electronic debit transactions;

(ii) Monitoring of the volume and value of its fraudulent electronic debit transactions;

(iii) Appropriate responses to suspicious electronic debit transactions in a manner designed to limit the costs to all parties from and prevent the occurrence of future fraudulent electronic debit transactions;

(iv) Methods to secure debit card and cardholder data; and

(v) Such other factors as the issuer considers appropriate.

(3) An issuer must review, at least annually, its fraud-prevention policies and procedures, and their implementation and update them as necessary in light of –

(i) their effectiveness in reducing the occurrence of, and cost to all parties from, fraudulent electronic debit transactions involving the issuer;

(ii) their cost-effectiveness; and

(iii) changes in the types of fraud, methods used to commit fraud, and available methods for detecting and preventing fraudulent electronic debit transactions that the issuer identifies from—

(A) its own experience or information;

(B) information provided to the issuer by its payment card networks, law enforcement agencies, and fraud-monitoring groups in which the issuer participates; and

(C) applicable supervisory guidance.

(c) *Notification.* To be eligible to receive or charge a fraud-prevention adjustment, an issuer must annually notify its payment card networks that it complies with the standards in paragraph (b).

(d) *Change in Status.* An issuer is not eligible to receive or charge a fraud-prevention adjustment if the issuer is substantially non-compliant with the standards set forth in paragraph (b), as determined by the issuer or the appropriate agency under § 235.9. Such an issuer must notify its payment card networks that it is no longer eligible to receive or charge a fraud-prevention adjustment no later than 10 days after determining or receiving notification from the appropriate agency under § 235.9 that the issuer is substantially non-compliant with the standards set forth in paragraph (b). The issuer must stop receiving and charging the fraud-prevention adjustment no later than 30 days after notifying its payment card networks.

Appendix A – Official Board Commentary on Regulation II

* * * * *

Section 235.4 Fraud-prevention adjustment

4(a) *[Reserved]*

4(b)(1) *Issuer standards*

1. An issuer's policies and procedures should address fraud related to debit card use by unauthorized persons. Examples of use by unauthorized persons include, but are not limited to, the following:

i. A thief steals a cardholder's wallet and uses the debit card to purchase goods, without the authority of the cardholder.

ii. A cardholder makes a purchase at a merchant. Subsequently, the merchant's employee uses information from the debit card to initiate a subsequent transaction, without the authority of the cardholder.

iii. A hacker steals cardholder account information from the issuer or a merchant processor and uses the stolen information to make unauthorized card-not-present purchases or to create a counterfeit card to make unauthorized card-present purchases.

2. An issuer's policies and procedures must be designed to reduce fraud, where cost effective, across all types of electronic debit transactions in which its cardholders engage. Therefore, an issuer should consider whether its policies and procedures are effective for each method used to authenticate the card (e.g., a chip or a code embedded in the magnetic stripe) and the cardholder (e.g., a signature or a PIN), and for different sales channels (e.g., card-present and card-not-present).

3. An issuer's policies and procedures must be designed to take effective steps to reduce both the occurrence of and costs to all parties from fraudulent electronic debit transactions. An issuer should take steps reasonably designed to reduce the number and value of its fraudulent electronic debit transactions relative to its non-fraudulent electronic debit transactions. These steps should reduce the costs from fraudulent transactions to all parties, not merely the issuer. For example, an issuer should take steps to reduce the number and value of its fraudulent electronic debit transactions relative to its non-fraudulent transactions whether or not it bears the fraud losses as a result of regulations or network rules.

4. For any given issuer, the number and value of fraudulent electronic debit transactions relative to non-fraudulent transactions may vary materially from year to year. Therefore, in certain circumstances, an issuer's policies and procedures may be effective notwithstanding a relative increase in the transactions that are fraudulent in a particular year. However, continuing increases in the share of fraudulent transactions would warrant further scrutiny.

5. In determining which fraud-prevention technologies to implement or retain, an issuer must consider the cost-effectiveness of the technology, that is, the expected cost of the technology relative to its expected effectiveness in controlling fraud. In evaluating the cost of a particular technology, an issuer should consider whether and to what extent other parties will incur costs to implement the technology, even though an issuer may not have complete

information about the costs that may be incurred by other parties, such as the cost of new merchant terminals. In evaluating the costs, an issuer should consider both initial implementation costs and ongoing costs of using the fraud-prevention method.

6. An issuer need not develop fraud-prevention technologies itself to satisfy the standards in § 235.4(b). An issuer may implement fraud-prevention technologies that have been developed by a third party that the issuer has determined are appropriate under its own policies and procedures.

Paragraph 4(b)(2) *Elements of fraud-prevention policies and procedures*

1. *In general.* An issuer may tailor its policies and procedures to address its particular debit card program, including the size of the program, the types of transactions in which its cardholders commonly engage, fraud types and methods experienced by the issuer, and the cost of implementing new fraud-prevention methods in light of the expected fraud reduction.

Paragraph 4(b)(2)(i). *Methods to identify and prevent fraudulent debit card transactions.*

1. *In general.* Examples of policies and procedures reasonably designed to identify and prevent fraudulent electronic debit transactions include the following:

(i) Practices to help determine whether a card is authentic and whether the user is authorized to use the card at the time of a transaction. For example, an issuer may specify the use of particular authentication technologies or methods, such as dynamic data, to better authenticate a card and cardholder at the time of the transaction, to the extent doing so does not inhibit the ability of a merchant to direct the routing of electronic debit transactions for processing over any payment card network that may process such transactions. (*See* § 235.7 and commentary thereto.)

(ii) An automated mechanism to assess the risk that a particular electronic debit transaction is fraudulent during the authorization process (i.e., before the issuer approves or declines an authorization request). For example, an issuer may use neural networks to identify transactions that present increased risk of fraud. As a result of this analysis, the issuer may decide to decline to authorize these transactions. An issuer may not be able to determine whether a given transaction in isolation is fraudulent at the time of authorization, and therefore may have implemented policies and procedures that monitor sets of transactions initiated with a cardholder's debit card. For example, an issuer could compare a set of transactions initiated with the card to a customer's typical transactions in order to determine whether a transaction is likely to be fraudulent. Similarly, an issuer could compare a set of transactions initiated with a debit card and common fraud patterns in order to determine whether a transaction or future transaction is likely to be fraudulent.

(iii) Practices to support reporting of lost and stolen cards or suspected incidences of fraud by cardholders or other parties to a transaction. As an example, an issuer may promote customer awareness by providing text alerts of transactions in order to detect fraudulent transactions in a timely manner. An issuer may also report debit cards suspected of being fraudulent to their networks for inclusion in a database of potentially compromised cards.

Paragraph 4(b)(2)(ii). *Monitoring of the issuer's volume and value of fraudulent electronic debit transactions.*

1. Tracking its fraudulent electronic debit transactions over time enables an issuer to assess whether its policies and procedures are effective. Accordingly, an issuer must include policies and procedures designed to monitor trends in the number and value of its fraudulent electronic debit transactions. An effective monitoring program would include tracking issuer losses from fraudulent electronic debit transactions, fraud-related chargebacks to acquirers, losses passed on to cardholders, and any other reimbursements from other parties. Other reimbursements could include payments made to issuers as a result of fines assessed to merchants for noncompliance with Payment Card Industry (PCI) Data Security Standards or other industry standards. An issuer should also establish procedures to track fraud-related information necessary to perform its reviews under § 235.4(b)(3) and to retain and report information as required under § 235.8.

Paragraph 4(b)(2)(iii). *Appropriate responses to suspicious electronic debit transactions.*

1. An issuer may identify transactions that it suspects to be fraudulent after it has authorized or settled the transaction. For example, a cardholder may inform the issuer that the cardholder did not initiate a transaction or transactions, or the issuer may learn of a fraudulent transaction or possibly compromised debit cards from the network, the acquirer, or other parties. An issuer must implement policies and procedures designed to provide an appropriate response once an issuer has identified suspicious transactions to reduce the occurrence of future fraudulent electronic debit transactions and the costs associated with such transactions. The appropriate response may differ depending on the facts and circumstances, including the issuer's assessment of the risk of future fraudulent electronic debit transactions. For example, in some circumstances, it may be sufficient for an issuer to monitor more closely the account with the suspicious transactions. In other circumstances, it may be necessary to contact the cardholder to verify a transaction, reissue a card, or close an account. An appropriate response may also require coordination with industry organizations, law enforcement agencies, and other parties, such as payment card networks, merchants, and issuer or merchant processors.

Paragraph 4(b)(2)(iv). *Methods to secure debit card and cardholder data.*

1. An issuer must implement policies and procedures designed to secure debit card and cardholder data. These policies and procedures should apply to data that are transmitted by the issuer (or its service provider) during transaction processing, that are stored by the issuer (or its service provider), and that are carried on media (e.g., laptops, transportable data storage devices) by employees or agents of the issuer. This standard may be incorporated into an issuer's information security program, as required by Section 501(b) of the Gramm-Leach-Bliley Act.

Paragraph 4(b)(3) *Review of and updates to policies and procedures.*

1. i. An issuer's assessment of the effectiveness of its policies and procedures should consider whether they are reasonably designed to reduce the number and value of fraudulent electronic debit transactions relative to non-fraudulent electronic debit transactions and are cost effective. (*See* comment 4(b)(1)-3 and comment 4(b)(1)-5).

ii. An issuer must also assess its policies and procedures in light of changes in fraud types (e.g., the use of counterfeit cards, lost or stolen cards) and methods (e.g., common purchase patterns indicating possible fraudulent behavior), as well as changes in the available methods of detecting and preventing fraudulent electronic debit transactions (e.g., transaction monitoring, authentication methods) as part of its periodic review of its policies and procedures. An issuer's review of its policies and procedures must consider information from the issuer's own experience and that the issuer otherwise identified itself; information from payment card networks, law enforcement agencies, and fraud-monitoring groups in which the issuer participates; and supervisory guidance. For example, an issuer should consider warnings and alerts it receives from payment card networks regarding compromised cards and data breaches.

2. An issuer should review its policies and procedures and their implementation more frequently than annually if the issuer determines that more frequent review is appropriate based on information obtained from monitoring its fraudulent electronic debit transactions, changes in the types or methods of fraud, or available methods of detecting and preventing fraudulent electronic debit transactions. (*See* § 235.4(b)(1)(ii) and commentary thereto.)

3. In light of an issuer's review of its policies and procedures, and their implementation, the issuer may determine that updates to its policies and procedures, and their implementation, are necessary. Merely determining that updates are necessary does not render an issuer ineligible to receive or charge the fraud-prevention adjustment. To remain eligible to receive or charge a fraud-prevention adjustment, however, an issuer should develop and implement such updates as soon as reasonably practicable, in light of the facts and circumstances.

4(c) *Notification.*

1. Payment card networks that plan to allow issuers to receive or charge a fraud-prevention adjustment can develop processes for identifying issuers eligible for this adjustment. Each issuer that wants to be eligible to receive or charge a fraud-prevention adjustment must notify annually the payment card networks in which it participates of its compliance through the networks' processes.

By order of the Board of Governors of the Federal Reserve System, July 27, 2012.

Robert deV. Frierson (signed)

Robert deV. Frierson,
Secretary of the Board.