FEDERAL REGISTER

Vol. 76 Wednesday,
No. 139 July 20, 2011

Part III

Federal Reserve System

12 CFR Part 235
Debit Card Interchange Fees and Routing; Interim Final Rule

FEDERAL RESERVE SYSTEM

12 CFR Part 235

[Regulation II; Docket No. R–1404]

RIN 7100–AD 63

Debit Card Interchange Fees and Routing

AGENCY: Board of Governors of the Federal Reserve System.

ACTION: Interim final rule; request for public comment.

SUMMARY: The Board is adopting an interim final rule and requesting comment on provisions in Regulation II (Debit Card Interchange Fees and Routing) adopted in accordance with Section 920(a)(5) of the Electronic Fund Transfer Act, which governs adjustments to debit interchange transaction fees for fraud-prevention costs. The provisions allow an issuer to receive an adjustment of 1 cent to its interchange transaction fee if the issuer develops, implements, and updates policies and procedures reasonably designed to identify and prevent fraudulent electronic debit transactions; monitor the incidence of, reimbursements received for, and losses incurred from fraudulent electronic debit transactions; respond appropriately to suspicious electronic debit transactions so as to limit the fraud losses that may occur and prevent the occurrence of future fraudulent electronic debit transactions; and secure debit card and cardholder data. If an issuer meets these standards and wishes to receive the adjustment, it must certify its eligibility to receive the fraud-prevention adjustment to the payment card networks in which the issuer participates.

DATES: The interim final rule is effective October 1, 2011.

Comment Period: Comments must be submitted by September 30, 2011.

ADDRESSES: You may submit comments, identified by Docket No. R–1404 and RIN No. 7100 AD 63, by any of the following methods:

Agency Web Site: http://www.federalreserve.gov. Follow the instructions for submitting comments at *http://www.federalreserve.gov/generalinfo/foia/ProposedRegs.cfm.*

Federal eRulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.

E-mail: regs.comments@federalreserve.gov. Include the docket number in the subject line of the message.

Fax: (202) 452–3819 or (202) 452–3102.

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

You must use only one method when submitting comments. All public comments are available from the Board's Web site at *http://www.federalreserve.gov/generalinfo/foia/ProposedRegs.cfm* as submitted, unless modified for technical reasons. Accordingly, your comments will not be edited to remove any identifying or contact information.

Public comments may also be viewed electronically or in paper in Room MP–500 of the Board's Martin Building (20th and C Streets, NW.) between 9 a.m. and 5 p.m. on weekdays.

FOR FURTHER INFORMATION CONTACT: Dena Milligan, Attorney (202/452–3900), Legal Division, David Mills, Manager and Economist (202/530–6265), Division of Reserve Bank Operations & 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, NW., 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. 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 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. 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. The Board has separately adopted a final rule implementing standards for assessing whether interchange transaction fees meet the requirements of Section 920(a) and establishing rules regarding routing choice and network exclusivity required by Section 920(b).[1]

Under EFTA Section 920(a)(5), the Board may allow for an adjustment to an interchange transaction fee amount 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 received from consumers, merchants, or payment card networks (including amounts from chargebacks) 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.[2]

In issuing the standards and prescribing regulations for the adjustment, the Board must 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 transaction fees have in the past reduced or increased incentives for

[1] Regulation II (published elsewhere in the **Federal Register**), 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.

[2] Regulation II defines electronic debit transaction (or ''debit card transaction'') to mean the use of a debit card (which includes a general-use prepaid card), by a person as a form of payment in the United States to initiate a debit to an account. This term does not include transactions initiated at an automated teller machine (ATM), including cash withdrawals and balance transfers initiated at an ATM.

parties involved in electronic debit transactions to reduce fraud on such transactions; and (7) such other factors as the Board considers appropriate.

II. Outreach and Information Collection

Following the enactment of the Dodd-Frank Act, the Board gathered information about fraud-prevention programs in the debit card industry in several ways. Board staff held numerous meetings with debit card issuers, payment card networks, merchant acquirers, merchants, industry trade associations, and consumer groups to discuss these programs. Topics discussed in those meetings included technological innovation in fraud prevention, fraud loss allocation among parties to electronic debit transactions, and fraud risk associated with different types of electronic debit transactions (*e.g.,* signature and PIN debit transactions).

In September 2010, the Board surveyed 131 bank holding companies and other financial institutions that, together with affiliates, have assets of $10 billion or more, and 16 payment card networks. As part of those surveys, the Board gathered information about the nature, type, and occurrence of fraud in electronic debit transactions; the losses due to fraudulent transactions absorbed by parties involved in those transactions; and the fraud-prevention and data-security activities and costs and related research and development costs (herein, collectively, referred to as fraud-prevention activities and costs) incurred by issuers in 2009.[3] From these surveys, the Board was able to estimate industry-wide fraud losses to all parties of a debit card transaction and to perform a more detailed analysis of fraud losses by type of authentication method (*e.g.,* PIN or signature). The survey data also provided an estimate of the loss allocation among parties to the transaction.[4]

III. Proposal

In December 2010, the Board requested comment on proposed Regulation II, Debit Card Interchange Fees and Routing.[5] As part of that proposal, the Board requested comment on two approaches to designing a framework for the fraud-prevention adjustment to the interchange transaction fee: A technology-specific approach and a non-prescriptive approach.[6] 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 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 a more general standard that an issuer must meet to be eligible to receive an adjustment for fraud-prevention costs.

The Board requested comment on various aspects of these approaches. For example, the Board requested information about the benefits and drawbacks of each approach, possible frameworks to implement the approaches, and the technologies or types of fraud-prevention activities whose costs should be considered under each approach. The Board also asked whether there were additional approaches that should be considered. Given survey data showing a substantially lower incidence of fraud for PIN debit transactions in comparison to signature-debit transactions, the Board also asked whether an adjustment should only be for PIN-based transactions.[7] The Board noted that comments received would be considered in the development of a specific proposal for further public comment.

IV. Overview of Comments and Interim Final Rule

The Board received numerous comments on the fraud-prevention adjustment from issuers, depository institution trade associations, payment card networks, merchants, merchant trade associations, individuals, consumer groups, technology companies, consultants, other government agencies, and members of Congress.

The comments were generally focused on four main topics: (1) Whether the overall framework for the adjustment should be technology-specific or non-prescriptive; (2) what form the fraud-prevention adjustment should take, *i.e.,* should the adjustment be tied to an eligible issuers' costs, perhaps up to a specific cap, or be uniform across eligible issuers; (3) whether the adjustment should apply only to particular authentication methods, such as for PIN-based authentication; and (4) the time frame for the effective date for the fraud-prevention adjustment. These comments are summarized below and are described in more detail in the Section Analysis.

Although there was not agreement on whether to pursue a technology-specific or non-prescriptive approach, commenters generally agreed that the Board should not mandate use of specific technologies. Merchant commenters generally favored the paradigm-shifting approach.[8] These commenters stated that the fraud-prevention adjustment should not cover costs associated with securing technologies that were known to be less effective at preventing fraud than other available technologies.[9]

In contrast, issuer commenters of all sizes and payment card networks preferred the non-prescriptive approach that would allow issuers to have the flexibility to tailor their fraud-prevention activities to address most effectively the risks they faced associated with 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.

In addition, among all types of commenters, there was a general consensus that the fraud-prevention adjustment should be effective at the same time as the interchange fee

[3] The surveys also requested information regarding the number of cards and accounts, the number and value of debit card transactions processed, interchange revenue received from networks, various costs associated with processing debit card transactions and operating a card program, and exclusivity arrangements and routing procedures.

[4] The Board reported preliminary survey results in the proposed rule (*See* 75 FR 81740–41, Dec. 28, 2010). Since that time, Board staff has further analyzed the data and addressed a number of minor problems, changing the number of usable responses. Fur example, some issuers provided fraud loss for certain types of fraud but did not report total fraud losses. In those instances, the sum of the reported fraud losses was used as that respondent's total fraud loss. In other instances, issuers misreported total fraud losses in a different field. Those totals were included in subsequent analysis of the data. In addition, prepaid fraud loss and fraud-prevention cost data have been included where appropriate. Therefore, in certain instances, some data reported in the initial proposal have changed. These data are reported separately (*see* ''2009 Interchange Revenue, Covered Issuer Cost, and Covered Issuer and Merchant Fraud Loss Related to Debit Card Transactions'' published on the Board's Web site at *http://www.federalreserve.gov*), and some data are discussed later in this notice.

[5] A final rule addressing other provisions in Regulation II is published elsewhere in the **Federal Register**.

[6] *See* 75 FR 81742–81743 (Dec. 28, 2010).

[7] Survey data shows that signature-debit fraud losses are approximately four times PIN-debit fraud losses.

[8] Merchants proposed a framework where an issuer receives an adjustment only if both the merchant and issuer use an eligible low-fraud technology.

[9] For example, merchant commenters argued that the fraud-prevention adjustment should not include activities aimed at securing signature debit transactions when PIN transactions are known to have lower incidence of fraud and lower average fraud loss per incident.

standard—either on July 21, 2011, or at a later date as suggested by some commenters. Many merchant commenters believed that the Board demonstrated that it had sufficient information to establish a fraud-prevention adjustment by the statutory effective date. Some commenters, particularly issuers and networks, argued that it was important to have the fraud-prevention adjustment in place alongside the rest of the interchange fee standards in order to avoid any gaps in the ability to fund certain fraud-prevention activities.

Under the interim final rule, if an issuer meets standards set forth by the Board, it may receive or charge a fraud-prevention 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, an issuer must 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. 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. Finally, the issuer must certify, on an annual basis, its compliance with the Board's standards to the payment card networks in which the issuer participates.[10]

The interim final rule will be effective concurrent with the interchange fee standard on October 1, 2011. Issuers must comply with the Board's fraud-prevention standards by that date in order to receive or charge the fraud-prevention adjustment to the interchange transaction fee on that date. The Board requests comment on all aspects of the interim final rule and will consider these comments in developing the final rule.

[10] The interim final rule applies to issuers and cards that are covered under the interchange fee standards. See discussion of the exemptions to the interchange fee standards in § 235.5 of Regulation II, Debit Card Interchange Fee and Routing—Final Rule, published elsewhere in the **Federal Register**.

V. Section Analysis

Section 235.4 sets forth the circumstances under which an issuer may receive or charge a fraud-prevention adjustment as an amount in addition to the amount permitted as an interchange transaction fee under § 235.3. Section 235.4 also prescribes the maximum amount of such adjustment.

A. 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. From the card issuer and network surveys, the Board estimates that industry-wide fraud losses to all parties of debit (including prepaid) card transactions were approximately $1.34 billion in 2009.[11] 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.[12]

The most commonly-reported and highest cost fraud types were counterfeit card fraud, lost and stolen card fraud, and mail, telephone, and Internet order (*i.e.,* card-not-present) fraud.[13] For signature and PIN debit card (including prepaid card) transactions combined, counterfeit card fraud represented 0.01 percent of all purchases transactions with an average loss of 2 cents per transaction and 4 basis points of transaction value. Lost and stolen card fraud was 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. Mail, telephone, and Internet order fraud was 0.01 percent of all purchase transactions with an average loss of 1 cent per transactions and 2 basis points of transaction value.

Extent to which the occurrence of fraud depends on authentication mechanism. The issuer survey data also provided information about the extent to which the occurrence of fraud depends on whether the transaction is authenticated with a signature or a PIN. 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.[14] 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. 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 almost 3 basis points of transaction value. Thus, on a per-dollar basis, signature debit fraud losses are approximately 4 times PIN debit fraud losses.[15]

The different fraud loss rates for signature and PIN transactions reflect, in part, differences in the ease of fraud associated with the two 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 only needs to steal information on the card in order to commit fraud.[16] In contrast, a PIN debit card transaction requires not only information contained on the card itself, but also something only the cardholder should know, namely the PIN. In this case, a thief generally needs both the information on the card and the cardholder's PIN to commit fraud.

Virtually all Internet debit card transactions are routed over signature

[11] 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 (including prepaid) 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.

[12] 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.

[13] Some issuers reported ATM fraud, which was excluded from fraud loss totals because ATM transactions are not defined in the statute or final rule as electronic debit transactions.

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

[15] 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.

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

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

The median amount spent by issuers on all reported fraud-prevention activities was approximately 1.8 cents per transaction. The most commonly reported fraud-prevention activity 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 transactions monitoring activity.[17]

Fraud-prevention costs expended by different parties. All parties to debit card transactions incur fraud-prevention costs. For example, some consumers routinely monitor their accounts for unauthorized debit card purchases; however, consumer costs are difficult to quantify. Some issuers, merchants, and acquirers pay networks, processors, or third-party vendors for fraud-prevention tools such as neural networks and access to databases about compromised cards and accounts. In addition to services they may purchase from others, merchants may develop their own fraud-prevention tools. For example, many large online merchants implement extra security measures to verify the legitimacy of a purchase. Typically these checks occur between the time a card is authorized by the issuer and the product is shipped to the purchaser. In their comments, 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, several merchants noted that these compliance costs can be substantial. As discussed more fully elsewhere in this notice, issuers incur costs for a variety of fraud-prevention activities.

Costs of fraudulent transactions absorbed by the different parties. Using the issuer survey data, the Board estimated the cost of fraudulent transactions absorbed by different parties to a debit card transaction. Based on the issuer survey responses, almost all of the reported fraud losses associated with debit card transactions fall on the issuers and merchants.[19] 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 distribution of fraud losses between issuers and merchants depends, in part, 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. In 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]

In general, merchants are subject to greater liability for fraud in card-not-present transactions than in card-present transactions. 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.[21]

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 for cardholders suggests that protecting 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 argued 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.

B. Section 235.4(a) Adjustment Amount

Section 235.4(a) permits an issuer to increase the amount of the interchange transaction fee it may receive or charge under § 235.3 by no more than 1 cent if the issuer complies with the standards in § 235.4(b). Section 235.4(a) does not differentiate the adjustment by authentication method or by type of transaction.[22]

1. Request for Comment and Comments Received

To inform its rulemaking, the Board's December 2010 proposal requested comment on whether the fraud-prevention adjustment should use the same implementation approach as the interchange fee standard; that is, either (1) An issuer-specific adjustment, with a safe harbor and a cap, or (2) a cap regardless of an issuer's costs. In a

[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* discussion of § 235.4(a) below.

[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 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] Most issuers reported that they offer zero or very limited liability to cardholders, in addition to the EFTA limits on consumer liability for unauthorized electronic fund transfers afforded to consumers, such that the fraud loss borne by cardholders is negligible. *See* 15 U.S.C. 1693g and 12 CFR 205.6. Payment card networks and merchant acquirers also reported very limited fraud losses for themselves.

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

[21] These percentages may differ from those noted in the Board's proposal (*See* 75 FR 81741, Dec. 28, 2010) because the number of usable survey responses has changed.

[22] For example, an issuer that complies with the fraud-prevention standards would be eligible to receive an interchange fee equal to the sum of the 21 cent base component, the 5 basis point *ad valorem* component, and the 1 cent fraud-prevention adjustment, equaling a total of 22 cents plus 5 basis points of the transaction's value for each electronic debit transaction.

related question, the Board also asked whether the adjustment should apply only to PIN-based transactions, in light of the fact that, as reported above in the statutory considerations section, signature debit fraud losses are approximately four times PIN debit fraud losses on a per-dollar basis.

In considering the implementation approach, many commenters referred to the statutory language that an adjustment should be ''reasonably necessary to make allowance for costs incurred by the issuer in preventing fraud in relation to electronic debit card transactions involving that issuer.'' They pointed to the term ''reasonably necessary'' as their basis for making arguments both for and against a cap on the amount of the adjustment. For example, most merchant commenters argued that it would be reasonably necessary for individual issuers to recover their initial capital costs for certain technologies, up to a cap equal to the cost associated with PIN debit card fraud-prevention activities.[23] They supported a process where issuers offered technologies with fraud loss rates lower than that for PIN debit transactions and merchants could choose whether or not to adopt these technologies. One merchant commenter opposed both a fixed amount and a cap as being counter to fair market price negotiation between the issuers offering technologies and merchants choosing to adopt these technologies. This commenter also argued that allowing recovery up to a cap ignored the statutory language to make allowance for costs ''incurred by the issuer'' and that the relevant cost measure should be an individual issuer's costs.

On the other hand, several issuer, network, and depository institution trade association commenters opposed a cap on the basis that it limited the recovery of costs that could be determined to be reasonably necessary to prevent fraud. Some of these commenters noted that any cap might reduce incentives to invest in innovative fraud-prevention techniques. A few of them supported a safe harbor to reduce compliance and supervisory burden and to encourage effective fraud prevention.

In response to the Board's question regarding whether a fraud-prevention adjustment should be only for PIN debit transactions, merchant commenters highlighted the survey data indicating that signature-debit transactions experience higher average fraud losses than PIN-debit transactions. They expressed a concern that, in the past, interchange fees supported incentives for issuers to promote a less secure form of authentication. Both issuer and merchant commenters acknowledged that some types of sales environments preclude use of PIN authentication. However, merchant commenters asserted that, when signature and PIN methods are available both on the card and at the sales terminal, issuers often encourage cardholders to route the transaction using their signature rather than their PIN so that issuers could receive higher interchange revenue.

A few issuers and networks commented that an adjustment only for PIN-based transactions would limit incentives to invest in potentially more effective authentication methods, such as dynamic data, that might not require a PIN. Some issuers commented that a fraud-prevention adjustment only for PIN debit transactions may limit fraud-prevention investments for non-PIN transactions, making these transactions less secure. According to these commenters, issuers may manage this risk by assessing cardholder fees on non-PIN transactions or by limiting the value allowed per transaction. These practices, asserted some issuers, may reduce sales or increase payment costs, especially for merchants that do not accept PIN debit cards. Merchant commenters, on the other hand, urged the Board to consider an adjustment only for technologies or methods with fraud loss rates lower than the rate for PIN debit card programs. These commenters argued that debit card transactions authorized with a PIN have a much lower fraud loss rate than those authorized with a signature. In particular, merchants did not want issuers to be reimbursed for efforts to better secure an inherently less secure authentication method.

2. Interim Final Rule

Section 920(a)(5) permits the Board to allow an adjustment to the amount of an interchange fee that an issuer may receive 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.'' Section 920(a)(5) of the EFTA does not specify what amount, or range of amounts, is considered ''reasonably necessary to make allowance for'' an issuer's fraud-prevention costs. The phrasing ''reasonably necessary to make allowance for'' fraud-prevention costs does not require a direct connection between the fraud-prevention adjustment and actual issuer costs; the statute requires only that the adjustment be ''reasonably necessary'' and ''make an allowance for'' fraud-prevention costs. Moreover, the statute does not require the Board to set the adjustment so that each (or any) issuer fully recovers its fraud-prevention costs. Instead, the statute provides for an ''allowance for'' fraud-prevention costs. The Board believes that an amount that makes allowance for an issuer's fraud-prevention costs is one that gives consideration to those costs, and allows a reasonable recovery of those costs based on the considerations in Section 920(a)(5)(B)(ii) described above.[24]

The statute also allows the Board, in setting a fraud-prevention adjustment, to consider such other factors as the Board considers appropriate.[25] As explained below, the Board has considered the fraud-prevention costs of parties to electronic debit transactions, the incentives created by the adjustment, and other factors in setting the adjustment.

The Board considered the fraud-prevention costs incurred by all parties to an electronic debit transaction: Consumers, merchants, payment card networks, processors, and issuers. The Board narrowed its focus to costs expended by merchants and issuers because most fraud-prevention costs are ultimately borne by these parties, and the fraud-prevention adjustment to the interchange transaction fee is effectively paid by merchants to issuers.

The Board recognizes that both merchants and issuers incur costs associated with fraud prevention including, for example, costs to comply with PCI–DSS and network rules related to fraud prevention. In addition, several merchant commenters stated that they, like issuers, have natural incentives to protect customer information and to safeguard their reputations as careful trustees of this information. To maintain these reputations and to reduce their exposure to fraud losses, these commenters noted that they have made substantial investments in fraud-prevention measures, including, as one online merchant noted, analysis of Internet Protocol address, Internet service provider, and device ID information.

For these reasons, the Board has adopted an interim final rule with a fraud-prevention adjustment set at issuer survey respondents' median fraud-prevention costs, minus those

[23] *See* comment from Merchants Payments Coalition.

[24] ''Allow for'' may be defined as ''to give consideration to circumstances or contingencies.'' *Merriam-Webster Dictionary* (''allow'' used with ''for'') (online edition).

[25] *See* EFTA Section 920(a)(5)(B)(ii)(VII).

fraud-prevention costs that are already part of the interchange fee standards.[26] The median issuer's per-transaction fraud-prevention cost as reported in response to the Board's survey is 1.8 cents. In its final rule for the interchange fee standards, the Board has included costs of transaction-monitoring systems that are integral to the authorization of a transaction in its setting of the interchange transaction fee standards. 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, they are excluded from the costs used to determine the fraud-prevention adjustment.[27] Issuers were instructed to separately report the costs of each type of fraud-prevention activity to the extent possible, and 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 fraud-prevention cost of 1.8 cents less the median transactions-monitoring cost of 0.7 cents, rounded to the nearest cent.

The median of the remaining fraud-prevention costs provides some issuers with recovery of all of these costs and other issuers with recovery of some of these costs. The Board believes that the median allowance helps to offset the costs of implementing activities that are effective at reducing fraud losses while placing cost discipline on issuers to ensure that those fraud-prevention activities are also cost effective and recognizing that fraud-prevention costs are incurred by both merchants and issuers. An issuer that meets the Board standards (discussed below) may receive the adjustment, even if its fraud-prevention costs are below the median, and no issuer may receive more than the median, regardless of its fraud-prevention costs.

The Board is concerned that limiting an adjustment to authentication methods available today, or a subset of those methods, may not allow flexibility for issuers to develop other methods of authentication that may be more effective than today's alternatives and may not require a PIN. It may also reduce the incentives for issuers to improve fraud-prevention techniques for systems that, for a variety of reasons, experience higher fraud rates. Further, the interchange fee standards set a maximum permissible interchange fee that an issuer may receive for electronic debit transactions, irrespective of authentication method. Because issuers are less likely to receive a higher interchange fee for signature-based transactions, issuer processing costs for PIN debit transactions are generally less than those for signature debit transactions, and fraud losses are significantly lower for PIN debit transactions than for signature debit transactions, 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.

For these reasons, the Board has adopted a fraud-prevention adjustment that is the same for each type authentication method.

C. Section 235.4(b)—Adoption of Non-Prescriptive Standards

1. Request for Comment and Comments Received

As discussed above, the Board's proposed rule did not contain a specific proposal for the fraud-prevention adjustment. Instead, the Board requested comment on two general approaches to the adjustment: A technology-specific approach and a non-prescriptive approach. The technology-specific approach was described as allowing issuers to recover some or all of its costs, perhaps up to a cap, incurred for implementing major innovations that would likely result in substantial reductions in fraud losses. As described in the proposed rule, the Board would identify paradigm-shifting technologies that would reduce debit card fraud in a cost-effective manner. The Board noted this approach might help spur adoption of technologies eligible for a fraud-prevention adjustment. At the same time, it might also reduce issuer incentives to invest in more effective and less costly technologies not identified by the Board.

Although neither merchant nor issuer commenters supported the Board mandating specific technologies, merchants and their trade associations preferred the technology-specific approach. Many merchants proposed that issuers be required to make specific technologies available to merchants that reduce fraud losses to a level lower than that associated with PIN debit transactions. They asserted that their proposal allowed the market, and not the Board, to determine technologies that are eligible for a fraud-prevention adjustment.[28] A merchant commenter suggested that this test could be further conditioned based on the riskiness of particular merchants. For example, the calculation of the fraud-prevention adjustment could consider the rate of fraud-related chargebacks to merchants, and those merchants with higher rates would pay a higher fraud-prevention adjustment than would those with lower rates, still up to a cap. One commenter noted that a metrics-based approach could be applied at the issuer level rather than at the technology level. For example, only issuers with a rate of fraud losses lower than the industry average may be eligible to receive or charge a fraud-prevention adjustment.

Alternatively, the non-prescriptive approach would entail a more general set of standards that an issuer must meet to be eligible to receive an adjustment for fraud-prevention costs. Such standards could require issuers to take steps reasonably necessary to maintain an effective fraud-prevention program but not prescribe specific technologies that must be employed as part of the program. This approach maintains issuer flexibility in responding to emerging and changing fraud risks.[29]

In their comments, issuers of all sizes, depository institution trade associations, payment card networks, and a federal regulatory agency preferred the non-prescriptive approach for a variety of reasons. Many of these commenters argued that debit card fraud is dynamic and requires issuers and networks to innovate on an ongoing basis in order to develop new responses to existing and emerging fraud risks. The flexibility to develop creative and timely responses, they noted, is important for detecting and preventing debit card fraud. Moreover, several of these commenters noted that the industry is better positioned than the Board to adapt fraud-prevention programs in a timely manner to respond effectively to changing fraud patterns.[30]

[26] The fraud-prevention adjustment does not include an allowance for fraud losses. EFTA Section 920(a)(5)(A)(i) limits the adjustment to ''costs incurred by the issuer in preventing fraud.'' Fraud losses are not costs incurred to prevent fraud. The Board includes issuer fraud losses as a basis for the establishment of the interchange fee standards in § 235.3 of the final rule. *See* notice elsewhere in the **Federal Register.**

[27] The median cost of fraud-prevention activities tied to authorization is about 0.7 cents.

[28] *See* letter from Merchants Payments Coalition. Although the Merchants Payments Coalition did not propose that the Board identify technologies in its standards, it did propose that any technologies issuers want to offer to merchants undergo an application and approval process, including a public comment period, managed by the Board.

[29] For a more detailed description of the two approaches proposed by the Board, see 75 FR 81742–81743 (Dec. 28, 2010).

[30] A few commenters, primarily technology vendors, consultants, and technology associations,

Continued

Many of these commenters expressed concerns with the identification, in any context, of particular technologies eligible for a fraud-prevention adjustment under a possible technology-specific approach. For example, several commenters suggested that this approach assumes that a single or limited set of technologies is more effective at reducing fraud losses than implementing a variety of technologies, practices, and methods in combination. To the extent that a set of technologies is identified, these commenters believed issuers would most likely invest in the set of technologies for which they can recover their costs. As a result, they asserted, competition among issuers (and networks) in fraud prevention will most likely be reduced. These commenters also echoed a concern noted by the Board in its December 2010 proposal—a risk that issuers would underinvest in new, non-eligible technologies, which may be more effective and less costly than those identified in the standard. Finally, a few of these commenters suggested that defining a list of eligible technologies would provide valuable information to fraudsters in their efforts to weaken mechanisms designed to strengthen security in the payment system. According to these commenters, such a list would also provide fraudsters with a good sense of the technologies most likely to be adopted, if they were not already, by the industry. Ultimately, these commenters argued that this information could make technologies that have been identified less effective over the long term.

2. Non-Prescriptive Approach

EFTA Section 920(a)(5) states that the Board's standards must require an issuer to take effective steps to reduce the occurrence of, and costs from, fraudulent electronic debit transactions and must ensure that an issuer implement ''cost-effective'' fraud-prevention technologies. As explained below, the Board is adopting standards for assessing whether the fraud-prevention program for an issuer is designed to reduce fraudulent debit card activity effectively. In assessing whether a program is effective, the Board does not believe that Section 920(a)(5) requires that the program prevent all fraud in order for an issuer to qualify for the fraud-prevention adjustment.

The dynamic nature of the debit card fraud environment requires standards that permit issuers to determine themselves the best methods to detect, prevent, and mitigate fraud losses for the size and scope of their debit card program and to respond to frequent changes in fraud patterns. Standards that incorporate a technology-specific approach do not provide sufficient flexibility to issuers to design and adapt policies and procedures that best meet a particular issuer's needs and that would most effectively reduce fraud losses for all parties to a transaction.

A variety of factors may affect the incidence of fraudulent electronic debit transactions and losses from those transactions, not all of which can be addressed solely by actions taken by issuers. For example, an acquirer or merchant processor used by merchants frequented by an issuer's cardholders may experience a data breach that increases the number of fraudulent transactions and losses for an issuer. An issuer's policies and procedures, however, may be able to mitigate the occurrence of, and costs from, fraudulent electronic debit transactions resulting from such a data breach. In this circumstance, an issuer's fraud-prevention policies and procedures may be effective, notwithstanding the fact that the issuer may have incurred a higher incidence of fraudulent electronic debit transactions than in more typical years.

Another factor affecting fraud trends is the nature of the fraud environment as a ''cat and mouse'' game. For example, as new and more effective fraud-prevention practices are employed by issuers, these practices will become targets for fraudsters wanting to compromise card and cardholder data. As technologies become less effective because of these efforts by fraudsters, issuers will be expected to find new ways to strengthen their fraud-prevention measures. To encourage improvement in fraud-prevention efforts, the interim final rule requires an issuer to review its policies and procedures, at least annually, and update them to address changes in the prevalence and nature of fraudulent electronic debit transactions and available fraud-prevention methods.

Specifying, and limiting the set of, technologies for which issuers recover their costs may weaken the long-term effectiveness of these technologies. For example, the risk that fraudsters may use this list as a way to focus their efforts to compromise card and cardholder data is material. For these reasons, the Board is adopting as an interim final rule, and requesting comment on, a non-prescriptive approach for the fraud-prevention adjustment. The Board invites public comment on all aspects of the interim final rule, including the questions specifically raised throughout the notice, and will adjust the rule as appropriate after consideration of comments received.

3. Develop and Implement Policies and Procedures

Section 235.4(b)(1) requires that in order to be eligible to receive a fraud-prevention adjustment, an issuer must 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 may include practices, activities, methods, or technologies that are used to implement and make effective an institution's fraud-prevention policies. Together, these policies and procedures shall be reasonably designed to detect, prevent, and mitigate fraudulent electronic debit transactions and as provided for in § 235.4(b)(1)(i–iv). Comment 4(b)–1 clarifies that an issuer must both develop and implement effective policies and procedures.

Comment 4(b)–2 discusses the types of fraud that an issuer's policies and procedures should address. In its proposal, the Board did not include regulatory language to define ''fraudulent electronic debit transaction'' but suggested in the preamble 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.[31] This definition is derived from the EFTA's definition of ''unauthorized electronic fund transfer.'' (15 U.S.C. 1693a(11)). One commenter stated that the definition of ''fraud'' should be expanded to include so-called ''friendly fraud'' where the cardholder authorizes the transaction and later claims the transaction cardholder did not engage in the transaction.

In contrast to elsewhere in the EFTA, Section 920 uses the term ''fraud'' rather than ''unauthorized'' transaction. Accordingly, for purposes of Section 920(a)(5), fraud in relation to electronic debit transaction may encompass more

supported the Board mandating particular technologies, such as chip and PIN or biometrics.

[31] *See* 75 FR 81722, 81740 (Dec. 28, 2010).

than ''unauthorized'' use of the card. For example, a cardholder may authorize payment to a fraudulent or ''phony'' merchant that does not deliver the expected goods or services to the cardholder. Another transaction that could be considered fraudulent, as suggested by commenters, is one in which the cardholder authorized the transaction and received the goods or services, but subsequently alleges fraudulently that the cardholder never received the goods or services. The Board has considered the comments and believes that fraud in electronic debit transactions is broader than unauthorized use and that whether a transaction is in fact fraudulent will depend on the facts and circumstances of the transaction.

All types of fraud impose costs on system participants, and the issuer's costs associated with preventing all types of fraud may be considered when determining the fraud-prevention adjustment. Under the interim final rule, the policies and procedures that an issuer must implement in order to qualify for the fraud-prevention adjustment need not necessarily address types of fraud, such as authorized transactions with a fraudulent merchant, that issuers generally have very limited ability to control. The issuer may choose, however, to include policies and procedures to minimize such fraudulent transactions if it learns of a specific fraudulent merchant or scam that its cardholders have experienced or are likely to experience. In such cases, the issuer could, for example, alert its cardholders as to the existence of the particular fraud. The Board requests 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.

Comment 4(b)(1)(i)–1 provides examples of practices that may be part of an issuer's policies and procedures to identify and prevent fraudulent electronic debit transactions. Comment 4(b)(1)(i)–2 clarifies that an issuer should assess the effectiveness of different authentication methods used by its cardholders, including the rate of fraudulent transactions for each method and consider practices to encourage the use of more effective authentication methods. This comment also clarifies that issuers should monitor industry developments and consider adopting, where practical, new methods of authentication that are materially more effective than the methods currently used by its cardholders. The Board requests comment on whether an issuer's policies and procedures should require an issuer to assess whether its customer rewards or similar programs provide inappropriate incentives to use an authentication method that is demonstrably less effective in preventing fraud.

Comment 4(b)(1)(ii)–1 provides that an issuer must have policies and procedures designed to monitor the types, number, and value of its fraudulent electronic debit transactions. The issuer must also track its and its cardholders' losses from fraudulent electronic debit transactions, its fraud-related chargebacks to merchant acquirers, and reimbursements from other parties to the transaction.

Comment 4(b)(1)(iii)–1 provides that an issuer must implement appropriate responses to suspicious transactions or transactions likely to be fraudulent. The comment clarifies that the response may be different depending on the nature of the transaction and may require the issuer to coordinate with industry organizations, law enforcement agencies, and other parties to the transaction. Comment 4(b)(1)(iii)–2 clarifies that it is not an appropriate response for the issuer to merely shift the loss to another party, other than the party that committed the fraud.

Comment 4(b)(1)(iv)–1 provides that an issuer's policies and procedures should be designed to secure debit card and cardholder data that are transmitted to or from an issuer (or its service provider) during transaction processing, stored by the issuer (or its service provider), and carried on media by employees or agents of the issuer. The comment also notes that this standard may be incorporated into an issuer's information security program as required by Section 501(b) of the Gramm-Leach-Bliley Act.

4. Review and Update Policies and Procedures

Section 235.4(b)(2) requires that an issuer review and update its fraud-prevention policies and procedures as least annually. In certain circumstances, more frequent updates may be necessary if there are significant changes in fraud types, fraud patterns, or fraud-prevention techniques or technologies.

Comment 4(b)(2)–1 provides that an issuer should review and update its policies and procedures if a significant change occurs even if the issuer reviewed and updated its policies and procedures within the preceding year.

5. Section 235.4(c) Certification

Section 235.4(c) requires an issuer to certify to its payment card networks that its fraud-prevention standards comply with the Board's standards as provided for in § 235.4(b). Issuers that are eligible for the adjustment should certify their compliance annually to each payment card network in which the issuer participates that allows issuers to receive or charge a fraud-prevention adjustment to their interchange transaction fee as permitted under §§ 235.3 and 235.4. The Board expects that these payment card networks will develop their own processes for identifying issuers eligible for this adjustment. (*Se*e comment 4(c)–1.)

The Board requests comment on whether the rule should establish a consistent certification process and reporting period for an issuer to certify to a payment card network that the issuer meets the Board's fraud-prevention standards and is eligible to receive or charge the fraud-prevention adjustment.

Form of Comment Letters

Comment letters should refer to Docket No. R–1404 and RIN No. 7100 AD 63 and when possible, should use a standard typeface with a font size of 10 or 12, to enable the Board to convert text submitted in paper form to machine-readable form through electronic scanning that will facilitate automated retrieval of comments for review. Comments may be mailed electronically to *regs.comments@federalreserve.gov*.

Solicitation of Comments Regarding Use of ''Plain Language''

Section 772 of the Gramm-Leach-Bliley Act of 1999 (12 U.S.C. 4809) requires the Board to use ''plain language'' in all proposed and final rules published after January 1, 2000. The Board invites comment on whether the interim final rule is clearly stated and effectively organized, and how the Board might make the text of the rule easier to understand.

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 reviewed the interim 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.

The interim final rule contains requirements subject to the PRA. The collection of information required by this interim final rule is found in § 235.4 of Regulation II (12 CFR part 235). Under the interim 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 shall 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. An issuer must review its fraud prevention policies and procedures at least annually, and update them as necessary to address changes in prevalence and nature of fraudulent electronic debit transactions and available methods of detecting, preventing, and mitigating fraud. Finally, the issuer must certify, on an annual basis, its compliance with the Board's standards to the payment card networks in which the issuer participates. The interim final rule will be effective concurrent with the interchange fee standard on October 1, 2011.

The interim final rule would apply to issuers that, together with their affiliates, have consolidated assets of $10 billion. The Board estimates that there are 380 issuers [32] regulated by the Federal financial regulatory agencies required to comply with the recordkeeping and reporting provisions under § 235.4.

The Board estimates that the 380 issuers would 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 60,800 hours. On a continuing basis, the Board estimates issuers would 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 15,200 hours. The Board estimates 380 issuers would take, on average, 5 minutes to comply with the reporting provision under § 235.4(c) (annual certification), and estimates the annual reporting burden to be 32 hours. The total annual PRA burden for this information collection is estimated to be 73,032 hours.

Comments are invited 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. Comments on the collection of information should be sent to Cynthia Ayouch, Acting Federal Reserve Clearance Officer, Division of Research and Statistics, Mail Stop 95–A, Board of Governors of the Federal Reserve System, Washington, DC 20551, with copies of such comments sent to the Office of Management and Budget, Paperwork Reduction Project (7100–to be assigned), Washington, DC 20503.

Regulatory Flexibility Act

The Board incorporates by reference the final Regulatory Flexibility Act analysis published with the Board's Regulation II, published elsewhere in the **Federal Register**. That analysis applies to the Regulation II as a whole, including the fraud-prevention adjustment adopted in this interim final rule.

Administrative Procedure Act

The Administrative Procedure Act (APA), 5 U.S.C. 551 *et seq.,* generally requires public notice before promulgation of regulations. *See* 5 U.S.C. 553(b). Unless notice or a hearing is specifically required by statute, however, the APA also provides an exception ''when the agency for good cause finds (and incorporates the finding and a brief statement of reasons therefore in the rules issued) that notice and public procedure thereon are impracticable, unnecessary, or contrary to the public interest.'' 5 U.S.C. 553(b)(B).

As an initial matter, Section 920 of the EFTA, as amended by the Dodd-Frank Act, does not specifically require the Board to provide notice or a hearing with respect to this rulemaking. In addition, the Board finds that there is good cause to conclude that providing notice and an opportunity to comment before issuing this interim final rule would be contrary to the public interest. As noted above, the Board received numerous comments that addressed questions posed by the Board regarding the fraud-prevention adjustment to the interchange transaction fee. Among all types of commenters, there was a general consensus that the fraud-prevention adjustment should be effective at the same time as the interchange fee standard in order to prevent any gaps in the ability to fund certain fraud-prevention activities. Without adequate funding, fraud-prevention activities could be reduced, thereby causing harm to consumers, merchants, and issuers. Moreover, the Board's data gathering effort provided the Board with sufficient information to develop and make a fraud-prevention adjustment effective concurrent with the interchange fee standard. Consequently, the Board finds that use of notice and comment procedures before issuing these rules would not be in the public interest. Interested parties will still have an opportunity to submit comments in response to this interim final rule. The interim final rule may be modified accordingly.

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 is amending 12 CFR part 235 as follows:

PART 235—DEBIT CARD INTERCHANGE FEES AND ROUTING

■ 1. The authority citation for part 235 continues to read as follows:

Authority: 15 U.S.C. 1693o–2.

■ 2. Add § 235.4 to read as follows:

§ 235.4 Fraud–prevention adjustment.

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

(b) *Issuer standards.* To be eligible to receive the fraud-prevention adjustment, an issuer shall—

(1) Develop and implement policies and procedures reasonably designed to—

[32] 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, Office of Thrift Supervision, 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.

(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; and

(2) Review its fraud-prevention policies and procedures at least annually, and update them as necessary to address changes in prevalence and nature of fraudulent electronic debit transactions and available methods of detecting, preventing, and mitigating fraud.

(c) *Certification.* To be eligible to receive or charge a fraud-prevention adjustment, an issuer that meets the standards set forth in paragraph (b) of this section must certify such compliance to its payment card networks on an annual basis.

■ 3. Appendix A to part 235 is amended to add new Section 235.4 to read as follows:

Appendix A to Part 235—Official Board Commentary on Regulation II

* * * * *

Section 235.4 Fraud-Prevention Adjustment

4(b) Issuer Standards

1. *In general.* Section 235.4(b) does not specify particular policies and procedures that an issuer must implement. Rather, an issuer must determine which policies and procedures are reasonably designed to achieve the objectives set forth in the standards. An issuer's policies and procedures must include fraud-prevention technologies and other methods or practices reasonably designed to detect, prevent, and mitigate fraudulent electronic debit transactions. An issuer does not satisfy the standards in § 235.4(b) if it merely develops policies and procedures; the issuer also must implement those policies and procedures. Implementing an issuer's fraud-prevention policies and procedures should include training the issuer's employees and agents, as appropriate.

2. An issuer's policies and procedures should address, among other things, fraud related to debit card use by unauthorized persons, which is a type of fraud that can be effectively addressed by the issuer, as the entity with the direct relationship with the cardholder and that authorizes the transaction. Examples of use by unauthorized persons include 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 $100 purchase at a merchant. Subsequently, the merchant's employee uses information from the debit card to initiate a subsequent transaction for an additional $100, without the authority of the cardholder.

iii. A hacker steals cardholder account information from a merchant processor and uses that information to make unauthorized purchases of goods or services.

Paragraph 4(b)(1)(i). *Identify and prevent fraudulent debit card transactions.*

1. *In general.* An issuer shall develop and implement policies and procedures reasonably designed to identify and prevent fraudulent electronic debit transactions. These policies and procedures should include activities to prevent, detect, and mitigate fraud even if the costs of these activities are not recoverable as part of the fraud-prevention adjustment. The issuer's policies and procedures may include the following:

i. 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 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.

ii. 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 compromised cards.

iii. Practices to help determine whether a user is authorized to use the card at the time of a transaction. For example, an issuer may specify the use of particular technologies or methods, such as dynamic data, to better authenticate a cardholder at the point of sale.

2. *Review of authentication methods.* The 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, including a review of the rate of fraudulent transactions for each authentication method. If one method of authentication results in significantly lower fraud losses than other method(s) of authentication enabled on the issuer's debit cards, the issuer should consider practices to encourage its cardholders to use the more effective authentication method. It should also consider methods for reducing fraud related to the authentication method that experiences higher fraud rates. In addition, the issuer should monitor industry developments and consider adopting, where practical, new method(s) of authentication that are materially more effective than the methods currently available to its cardholders.

Paragraph 4(b)(1)(ii). *Monitor the incidence of, reimbursements received for, and losses incurred from fraudulent electronic debit transactions.*

1. In order to inform its policies and procedures, an issuer must be able to track its fraudulent electronic debit transactions over time. Accordingly, an issuer must have policies and procedures designed to monitor the types, number, and value of fraudulent electronic debit transactions. In addition, an issuer must track its and its cardholders' losses from fraudulent electronic debit transactions, its fraud-related chargebacks to acquirers, and any 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.

Paragraph 4(b)(1)(iii). *Respond 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 authorize 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 have policies and procedures in place designed to implement an appropriate response once an issuer has identified suspicious transactions or transactions likely to be fraudulent. The appropriate response is likely to differ depending on the circumstances and 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 reissue cards or close the 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. An appropriate response would be reasonably designed to mitigate fraud losses due to suspicious transactions and transactions alleged to be fraudulent across all parties to such transactions.

2. 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.

Paragraph 4(b)(1)(iv). *Secure debit card and cardholder data.*

1. An issuer must have policies and procedures designed to secure debit card and cardholder 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)(2) *Annual review*

1. *Periodic updates of policies and procedures.* In general, an issuer must review its policies and procedures at least annually. In certain circumstances, however, an issuer may need to review and update its policies and procedures more frequently than once a year. For example, during a particular year, there may be significant changes in fraud types, fraud patterns, or fraud-prevention methods or technologies. If a significant change occurs, an issuer must review and, if necessary, update its fraud-prevention policies and procedures to address the significant change, even if the issuer has reviewed its policies and procedures within the preceding year.

4(c) Certification.

1. To be eligible to receive the fraud-prevention adjustment, each issuer must certify its compliance with the Board's fraud-prevention standards to the payment card networks in which it participates on an annual basis. Payment card networks that plan to allow issuers to receive or charge a fraud-prevention adjustment will develop their own processes for identifying issuers eligible for this adjustment. An issuer need not certify if it chooses not to receive any fraud-prevention adjustment available through a network.

By order of the Board of Governors of the Federal Reserve System, June 30, 2011.

Jennifer J. Johnson,

Secretary of the Board.

[FR Doc. 2011–16860 Filed 7–19–11; 8:45 am]

BILLING CODE 6210–01–P