



February 22, 2011

By Electronic Delivery

Louise L. Roseman
Director, Division of Reserve Bank Operations and Payment Systems
Board of Governors of the Federal Reserve System
20th Street & Constitution Avenue NW
Washington, DC 20551

**Re: Docket No. R-1404 (Debit Card Interchange and Routing) & RIN No. 7100 AD63
Notice of Proposed Rulemaking, 12 C.F.R. Part 235**

Dear Ms. Roseman:

Dell, Inc. ("Dell") respectfully submits the following comments in response to the Notice of Proposed Rulemaking ("NPRM") issued by the Board of Governors of the Federal Reserve System (the "Board") pursuant to Section 920 of the Electronic Fund Transfer Act ("EFTA" or the "Act").

Dell appreciates the diligent work of the Board as reflected in the NPRM. The Board made a number of important determinations and substantial progress toward establishing regulations regarding debit card interchange that will constrain the market power that has harmed merchants like Dell over the years. In particular, Dell lauds the Board's proposed rules with respect to 12 C.F.R. § 235.3 regarding "reasonable and proportional" interchange fees, which on their face have the potential to eliminate the long-standing interchange and wholly unjustified price discrimination against card-not-present merchants, at least with respect to covered debit transactions.¹

Dell operates in the highly competitive consumer electronics market, a market with constant pressure to keep operating costs low and eliminate any conceivable inefficiencies. We operate a low margin business and it is our practice to identify and eliminate inefficiencies and pass along the benefits to the end consumer. Interchange is one such efficiency. We have no doubt that Dell will quickly pass the benefits of reduced interchange fees to our customers.

¹ Internet merchants, together with telephone, television, and mail-order merchants, are often referred to as "card-not-present" or CNP merchants. Although Dell objects to the term "card-not-present" because it has been used as a rationale to justify discriminatory interchange and chargeback rules, the term is used here for convenience.

We write to bring the Board's attention to two primary issues of concern to Internet and other card-not-present merchants.

- **Reasonable and Proportional Interchange Fees.** Reasonable interchange fees should be the same for card-present and card-not-present merchants. Because the costs of authorization, clearance, and settlement ("ACS") of these debit transactions are virtually the same, it necessarily follows that all merchants should pay the same basic rates of interchange to the extent such fees are necessary at all.
- **Fraud Adjustment.** The Board should adopt a non-prescriptive approach which allows issuers to qualify for a fraud adjustment to recover the capital investment costs of paradigm-shifting technologies. Eligibility would be determined by an analysis of the costs and amount of reduced fraud, and would require issuers to assume liability for fraud occurring on qualified technology. Any fraud standards must be based upon merchant fraud experience and must not discriminate based upon merchant type.

I. Historically, the Payment Industry Has Used Arbitrary Merchant Categories to Justify Interchange That Does Not Reflect Actual Costs

A. Market Power Has Allowed Payment Networks to Charge Card-Not-Present Merchants Double the Rate of Brick-and-Mortar Competitors

Since the Internet became a commonly used medium for commerce in the 1990s, the payment industry has required Internet merchants to pay vastly higher interchange rates than those paid by their direct competitors in traditional brick-and-mortar environments. These rates are some 98 basis points higher and more than double brick-and-mortar rates.²

Payment networks initially claimed that card-not-present transactions posed higher risks to the system which justified extraordinarily high interchange rates. If ever valid, that justification has vanished over time.³ Nor were these rates necessary to gain card acceptance, as the NPRM incorrectly observed.⁴ The introduction of higher rates for card-not-present merchants was purely the result of network market power over such merchants, who had no other viable alternative to major payment cards despite excessive

² See Visa U.S.A. Interchange Reimbursement Fees – October 2010, <http://usa.visa.com/download/merchants/october-2010-visa-usa-interchange-rate-sheet.pdf> (comparing "CPS/e-Commerce Basic" rate with "CPS/Retail Debit—Performance Threshold I" rate).

³ For example, overall fraud loss rates for Internet merchants have steadily declined over the last 11 years as measured by CyberSource (now a subsidiary of Visa). See CyberSource Online Fraud Report 2011 at 4, 5, 19.

⁴ The NPRM notes that, "Beginning in the early 1990s, signature debit networks also began creating separate categories for merchants in certain market segments (e.g., supermarkets and card-not-present transactions) to gain increased acceptance in those markets." NPRM at 81724. While this statement may be partly correct – with respect to supermarkets where lower rates were created to induce acceptance – it is incorrect with respect to card-not-present merchants that always paid higher discriminatory rates. These higher rates had nothing to do with inducing acceptance.

rates of interchange.⁵ Indeed, card-not-present debit interchange rates have increased over time despite higher volume (which continues to grow at double-digit rates) and the maturation of the Internet.⁶ As observed in the NPRM, today card-not-present transactions comprise fully 14% of signature debit transactions and 10% of debit transactions overall. NPRM at 81725 n.19.

B. Card-Not-Present Merchants Pay for the Vast Majority of Fraud

The inequities of this two-tier interchange system have been compounded by the fact that merchants bear most of the fraud and chargeback risks associated with card-not-present transactions through chargeback rules imposed by the payment networks.⁷ As a result, in addition to paying higher interchange fees than brick-and-mortar merchants, card-not-present merchants absorb the vast majority of the fraud costs associated with payment card transactions. The NPRM acknowledges this reality, noting that according to network and issuer surveys, merchants “assume approximately 76 percent of signature debit card fraud for card-not-present transactions.” NPRM at 81741.⁸

C. Internet Merchants Incur High Costs to Effectively Manage Risk

Further compounding this inequity, the higher interchange paid by card-not-present merchants penalizes high quality Internet merchants such as Dell that have developed, at great expense, their own risk management systems that rival (if not exceed) those utilized by issuers.⁹ This unjustified and discriminatory structure has remained

⁵ As observed in the NPRM, Internet retailers have no alternative technology that could cut merchant costs. NPRM at 81723; 81741 & n.70, 81749.

⁶ Price discrimination is classic indicia of market power. *See, e.g., In re Brand Name Prescription Drugs Antitrust Litig.*, 186 F. 3d 781, 783 (7th Cir. 1999) (“price discrimination implies market power”); *United States v. Visa U.S.A. Inc.*, 163 F. Supp. 2d 322, 340 (S.D.N.Y. 2001) (“Defendants’ ability to price discriminate also illustrates their market power.”); *In re Visa Check/MasterMoney Antitrust Litig.*, 192 F.R.D. 68, 74 (E.D.N.Y. 2000) (“Another test of market power is the ability to engage in price discrimination”).

⁷ Card-not-present merchants absorb approximately 80 percent of fraud chargebacks. Jane Adler, *Checking the Chargeback Scourge*, Digital Transactions at 36 (chart), 38 (June 2010), <http://www.digitaltransactions.net/files/DigitalTransactionsJune2010.pdf>; CyberSource Online Fraud Report 2011 at 17 (citing 22-23% rate of chargeback recovery). On top of all this, merchants are charged fees for every chargeback they represent, and pay additional fees if the chargeback is not reversed upon representment.

⁸ *See also* Richard J. Sullivan, *The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options*, Federal Reserve Bank of Kansas City, Economic Review 101, 111 (2d Qtr. 2010), <http://www.kansascityfed.org/Publicat/Econrev/pdf/10q2Sullivan.pdf> (noting that, “relative to their sales, card payment fraud losses fall most heavily on Internet, mail order, and telephone merchants because nearly all their payments are card-not-present transactions.”)

⁹ In its 2011 annual survey of online fraud, CyberSource (now owned by Visa) reports that one-third or more of merchants spend 0.5% or more of their online revenues to manage fraud. CyberSource Online Fraud Report 2011 at 21. CyberSource notes that “Online payment fraud impacts profits from online sales in multiple ways. Besides direct revenue losses, the cost of stolen goods/services and associated delivery/fulfillment costs, there are the additional costs of rejecting valid orders, staffing manual review, administration of fraud claims, as well as challenges associated with business scalability.” *Id.* at 6. Indeed, the cost of addressing a single chargeback is substantial: “The average time spent overall was 1.8 hours,

intact well over a decade after Internet commerce began to flourish, even though many Internet merchants have managed to drastically reduce fraud through significant investment in fraud management systems.

Established merchants like Dell have made substantial investments in fraud management systems, which has resulted in fraud rates that are equal to or better than many brick-and-mortar merchants. Yet these merchants continue to pay discriminatory interchange rates and bear the cost of most direct fraud loss. Accordingly, in our view any plausible interpretation of “reasonable and proportional” interchange would eliminate the discriminatory treatment of card-not-present merchants (at least with respect to debit transactions).

Dell’s success in preventing fraud is a result of its highly effective fraud prevention systems. In fact, overall Dell estimates that 1% of orders are fraudulent, and that the company detects and rejects 95% of these orders. Dell invested \$5.6 million over the past three years in fraud management, and incurs a \$1-2 million charge annually for its efforts.¹⁰ Over the same three year period, Dell stopped over \$201 million in fraudulent transactions *which had been authorized by issuers at checkout*.¹¹ Industry-wide, billions of dollars of fraudulent orders are rejected each year.¹²

The key to the Internet industry’s anti-fraud strategy is checking a potential transaction before shipment is executed. These checks typically occur after the issuer has authorized the transaction. Sophisticated Internet merchants create a series of automated

with a median time of 1 hour to handle a fraud chargeback (total time consumed for research, documentation, submission).” *Id.* at 17.

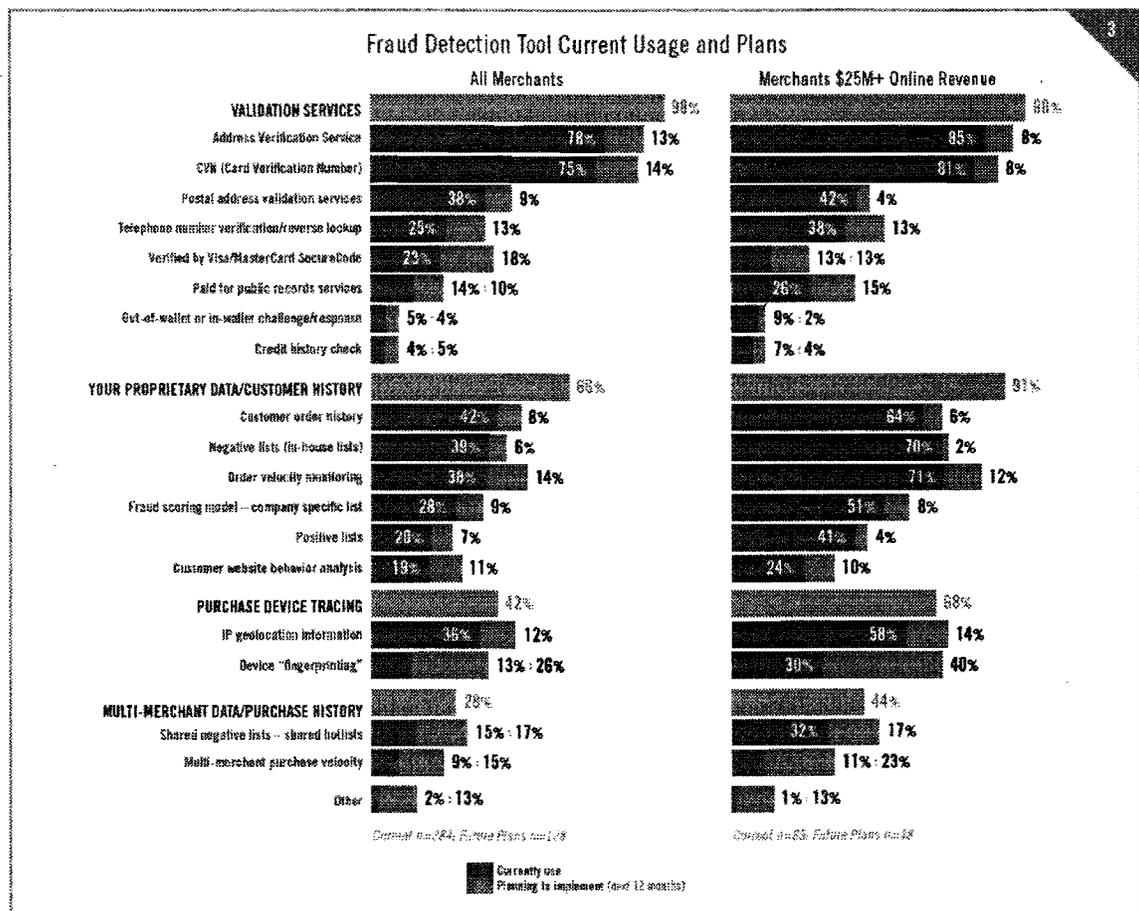
¹⁰ Industry-wide, Internet merchants spent 0.3% of their total sales on fraud protection expenses. See CyberSource Online Fraud Report 2010 at 21; Jane Adler, *Checking the Chargeback Scourge*, Digital Transactions at 34-35 (June 2010), <http://www.digitaltransactions.net/files/DigitalTransactionsJune2010.pdf>. Applied across the e-commerce market, Internet merchants spend some **\$816 million** annually for fraud protection. This estimate is based upon 0.3% of the \$272 billion market for online travel and retail, which is conservative because it excludes the sizeable numbers of Internet debit transactions relating to small business and digital download purchases. See U.S. Census Dep’t, Quarterly Retail E-Commerce Sales, (Aug. 17, 2010) (prior four quarters), <http://www.census.gov/retail/mrts/www/data/pdf/10q2.pdf> (non-travel online market, calculated by the Census Department to be approximately \$160 billion); *PhoCusWright’s U.S. Online Travel Overview Eighth Edition* (online travel market at \$112 billion); see also comScore Press Release, *comScore Reports Q2 2010 U.S. Retail E-Commerce Spending Up 9 Percent vs. Year Ago* (Aug. 10, 2010), http://comscore.com/Press_Events/Press_Releases/2010/8/comScore_Reports_Q2_2010_U.S._Retail_E-Commerce_Spending_Up_9_Percent_vs._Year_Ago (reporting \$135.5 billion non-travel retail over the prior four quarters).

¹¹ This estimate is based upon the number of Dell’s payment card transactions during 2007-2009, multiplied by 1% and by 95%.

¹² For example, the 334 merchants who participated in the 12th Annual CyberSource Online Fraud Report rejected 2.7% of orders overall. Based on reported revenues of \$65 billion, this amounts to approximately \$1.67 billion in orders rejected as fraudulent. CyberSource Online Fraud Report 2011 at 2, 5.

checks to determine the risk of a given transaction, and typically separate out up to 20% of those transactions for additional, manual review.¹³

The sophisticated Internet merchant's chain of analytical and risk assessment functions aims to limit the false negatives (valid transactions suspected of fraud and subject to loss if approval is delayed) and false positives (fraudulent transactions making it through fraud-prevention screening). The cost and complexity of these anti-fraud efforts can be seen throughout the transaction processing chain.¹⁴ Internet merchants collect and analyze an array of information about each transaction, including IP address, Internet Service Provider, and increasingly, device ID information. During manual review of suspicious transactions, more than half of larger Internet merchants use Google Maps and social networking sites to investigate suspicious transactions. The chart below displays the range of anti-fraud measures employed by Internet merchants.¹⁵



¹³ CyberSource Online Fraud Report 2011 at 5.

¹⁴ It is worth noting that brick-and-mortar merchants do not have these fraud detection capabilities. This reinforces the illogic of the current interchange system.

¹⁵ CyberSource Online Fraud Report 2011 at 8.

As dictated by the Act, a complete account of the fraud costs borne by Internet merchants must take all of these costs into account, as well as the extensive customer service investments sophisticated Internet merchants make to avoid chargebacks in the first place.

II. Congress Enacted the EFTA to Curb Network Market Power

That Congress intended to constrain the networks' (and issuers') market power over merchants is readily apparent from Section 920 of the EFTA as well as its legislative history.¹⁶ The Board correctly observed that although the Act "requires only the consideration" of a number of factors, these enumerated considerations are clearly "indicative of Congressional intent." *See* NPRM at 81734.

Nothing in the EFTA suggests Congress intended to allow variation in interchange fees by merchant category. In fact, sanctioning continued price discrimination – which is a classic example of a dysfunctional and failed market – would be antithetical to the fundamental purposes of the Act. Rather, Congress intended that only actual issuer ACS costs for particular transactions comprise a reasonable interchange fee. *See* NPRM at 81734. As discussed below, variations based upon merchant category may result in fees which are not "reasonable and proportional" to an issuer's ACS costs and which could reinstate the networks' exercise of market power over disfavored merchants, contrary to the EFTA. Because ACS costs are virtually the same for all merchants, the Board's final rulemaking should bar what the proposed Commentary calls "variation among interchange fees" unless such variation is tied to material differences in an issuer's actual, allowable ACS costs.

III. Reasonable Interchange Fees Are Virtually the Same for All Merchants

A. Variation Among Interchange Fees Should Be Prohibited Unless Tied to Issuer Costs

Variation among interchange fees by merchant category, particularly by card-present versus card-not-present distinctions, should not be allowed under any rule adopted by the Board. The NPRM discusses allowable costs, and the true ACS costs to issuers do not vary materially for card-not-present transactions. Indeed, the NPRM does not refer to any quantification of cost differences between the two types of transactions for issuers. However, Proposed Commentary 3(b)-4 (NPRM at 81759) and 3(b)-1

¹⁶ *See* 156 Cong. Rec. 156, S3696 (May 13, 2010) (Remarks of Sen. Durbin) ("Right now in the United States, there are zero transaction fees deducted when you use a check. The Federal Reserve does not allow transaction fees to be charged for checks. But when it comes to debit cards, Visa and MasterCard charge high interchange fees just as they do for credit. Why? Because they can get away with it. There is no regulation, there is no law, there is no one holding them accountable."); *see also* Andrew Martin, *How Visa, Using Card Fees, Dominates a Market*, N.Y. Times (Jan. 5, 2010), http://www.nytimes.com/2010/01/05/your-money/credit-and-debit-cards/05visa.html?_r=1.

(NPRM at 81760) allows for “variation among interchange fees” – including for card-not-present transactions – so long as fees remain below the safe harbor or cap. NPRM at 81736. In our view, such variation should not be permitted.

For Internet merchants, discriminatory interchange is simply an exercise of market power by the networks, particularly Visa and MasterCard – not a strategy deployed to increase acceptance or justified by actual increased costs to process card-not-present transactions. Indeed, the disparity in rates has only increased despite the increased volume and maturity and relative safety of the Internet channel with respect to merchants such as Dell. As the Board recognized, the Congressional intent behind the EFTA was to strictly limit these fees to the actual – and nominal – processing costs of issuers. NPRM at 81733-34.

Allowing variation of ACS costs for different types of merchants ignores the fact that properly defined, allowable ACS costs are virtually the same regardless of merchant category.¹⁷ As the Board is aware, the transaction messaging flow for debit transactions is identical for card-present and card-not-present transactions. NPRM at 81724. Without substantiation of purportedly higher and properly allowable ACS costs to issuers for particular card-not-present transactions, variation by type of merchant should not be permitted.

B. “Averaging” Across Issuer or Network Conflicts with the Act and Invites Continued Discrimination Against Internet Merchants

The Board requested comment on whether it should permit issuers or networks to exceed the thresholds if the issuer’s “average” transaction costs fell within the safe harbor or cap. NPRM at 81738-39. We are strongly opposed to this approach because it is simply a veiled invitation for the networks to set card-not-present rates above the cap and permit fees which are not reasonable or proportional to the cost incurred with respect to card-not-present transactions, in clear violation of the Act.¹⁸

¹⁷ For example, the identity of the transaction flow for card-present and card-not-present transactions can be seen in a 2003 publication of the Federal Reserve Bank of Kansas City, which presents several flowcharts setting forth “authorization,” “processing” and “settlement.” Terri Bradford et al., *Nonbanks in the Payments System*, 24-26 (Nov. 2003). In each chart, the messaging flows and processing steps for credit and signature debit (also known as “offline debit”) are the same for card-present and card-not-present transactions.

¹⁸ Indeed, the averaging proposal likely originated in comment letters from Visa and certain unidentified banks during the first phase of the Board’s rulemaking. See Letter from Visa to Federal Reserve Board (Nov. 8, 2010), http://www.federalreserve.gov/newsevents/files/visa_comment_letter_20101108.pdf; Letter from Oliver Ireland, Morrison Foerster LLP to Federal Reserve Board (Nov. 5, 2010), http://www.federalreserve.gov/newsevents/files/morrison_and_foerster_comment_letter_20101105.pdf (substantially similar letter, using much of the same language, submitted on behalf of “a number of institutions” which are not identified). These letters proposed averaging so that “a network could set different rates based on merchant size, merchant segment, acceptance channel (e.g., card present vs. card not present),” without any suggestion that these transactions varied in actual cost to issuers. (Visa Comment Letter at 18.) The letters were also careful to note that “[t]he Board would need to periodically update the Average Effective Debit Interchange Rate as the underlying aggregate issuer cost profiles

While the NPRM mentions the purported increased “flexibility” of this proposal, there is no discussion about what that means, let alone why flexibility in debit interchange rates is needed or consistent with the statute. The NPRM refers only to the ability to adjust pricing to “reflect differences in risk, among other things.” NPRM at 81738. Transaction risk concerns fraud, and as such should be addressed in the distinct rulemaking on any fraud adjustment – a rulemaking that, as the statute requires, must account for the cost of fraud to merchants, among others.¹⁹ To the extent this reference to risk relates to card-not-present merchants, it is worth noting that such merchants currently bear nearly all the risk of fraud, and thus charging them higher rates under the guise of “flexibility” and fraud risks cannot be justified.

For these reasons, an averaging approach will result in the continued imposition of excessive and unjustified interchange fees on Internet merchants. Differential rates also perpetuate the current structure, where high-quality merchants whose business is limited to card-not-present transactions subsidize low-quality merchants across all merchant categories.²⁰ As the Board recognizes, such an approach also conflicts with the text of the Act, which focuses on the costs to “the” particular issuer for “the” particular transaction – costs which do not vary by merchant type. NPRM at 81738.

Moreover, we share the Board’s concern that an averaging approach that requires an ex ante calculation of differential rates could result in the average exceeding the cap. This concern is aggravated by the possibility, if not the likelihood, that averaging based on ex ante calculations may understate actual card-not-present volumes (which are increasing and will continue to do so with mobile payments), thereby enabling the networks to continually overcharge merchants such as Dell. We see no easy corrective for this other than to require issuers to provide inherently unreliable growth forecasts for card-not-present transactions before each year and to rebate any such overcharges ex post. In short, in addition to being unprincipled, this approach will present difficulties in administration that the Board should avoid.²¹

C. The Board Should Adopt Alternative 1 with Its Potential for Lower Fees and the Express Definition of Allowable Costs

change over time” – thereby insuring that “average” costs would continue to rise with the growth of card-not-present transactions.

¹⁹ The Act’s separate fraud adjustment provision dictates that the Board broadly consider “the nature, type, and occurrence of fraud” in debit transactions, EFTA § 920(a)(5)(B)(ii)(I), and account for the liability of all parties for fraud loss and fraud prevention costs, EFTA § 920(a)(5)(B)(ii)(IV & V).

²⁰ It is important to note that low quality merchants that create risks for the system exist in both the physical and card-not-present environments.

²¹ If the Board were to allow averaging across networks or issuers, higher interchange rates should not be imposed upon all card-not-present merchants. Because low quality, high risk merchants exist in both environments, higher rates should be limited to those demonstrably higher-risk merchants, whether “card-not-present” or brick-and-mortar.

Dell supports the Board's proposed standard in 12 C.F.R. § 235.3 mandating that any interchange fee be "reasonable and proportional" to the cost incurred by the issuer for the transaction, albeit with lower thresholds.

1. Alternative 1 Properly Defines ACS Costs

The interchange fee standard proposed under Alternative 1, 12 C.F.R. § 235.3(c), most closely follows the text of the Act, which clearly contemplates an issuer-specific determination of ACS costs. *See* EFTA §920(a)(2) (interchange an issuer may receive with respect to an electronic debit transaction must be "reasonable and proportional to the cost incurred by the issuer with respect to the transaction").

As the NPRM notes, this alternative defines as allowable "only those costs that are specifically mentioned for consideration in the statute." NPRM at 81734-35. In contrast, the rules proposed for Alternative 2 do not define allowable costs. Although presumably the same definition of allowable costs would be used to make any adjustments to the fee cap in Alternative 2, we believe it is important that these definitions be part of the regulations. Limiting allowable costs to an issuer's role in authorization, clearance, and settlement – and explicitly defining such costs in § 235.3(c) – thus follows the intent of Congress and the plain text of the statute.

2. Issuer-Specific Cost Calculation May Result in Lower Interchange Fees, Whereas Under Alternative 2 Issuers Will Default to the Cap

Alternative 1's more flexible structure allows for variability in issuers' costs. Further, it could to some degree promote issuer competition to increase efficiency, particularly if issuers attempt to get below the safe harbor to increase their profits. As the NPRM notes, requiring issuers to demonstrate that their actual allowable costs exceed the safe-harbor provides an incentive to keep these costs below it. NPRM at 81738. Under Alternative 2, on the other hand, we believe it is likely that all issuers will charge the maximum 12 cents per transaction, and we see no reason why allowing issuers to default to that amount is the correct result from a statutory or policy perspective.

To the extent the Board believes that networks may set interchange rates below 12 cents to induce merchants to preferentially route to them by taking advantage of § 235.7, such an approach will be ineffective unless and until most merchants have multiple routing options, including those that accept only signature debit. Because PIN debit (or any other alternative) is not widely available over the Internet, card-not-present merchants will have little or no alternative under Alternative A to § 235.7, (*i.e.*, one signature and one PIN alternative) and little or no alternative until 2013 under Alternative B (two signature and two PIN alternatives). NPRM at 81753. And we cannot avoid noting that roughly 75% of merchants will have no routing alternative under Alternative A for the foreseeable future. That backdrop reinforces our view that Alternative 2 will result in issuers defaulting to 12 cents per transaction, a result that cannot be justified under the statute given that 12 cents substantially exceeds issuers' true ACS costs.

3. Interchange Fees Are Too High Under Either Alternative

Under either alternative to § 235.3, however, allowing issuer ACS costs of 12 or even 7 cents per transaction is too high. As the NPRM points out, the weighted average cost to issuers is actually 4 cents per transaction. NPRM at 81737. Average transaction cost is a more economically meaningful measure than median issuer cost. As other comments have pointed out, the true average cost is closer to 0.33 cents for PIN and 1.36 cents for signature.²² The true costs of ACS – “the three least expensive steps in the debit service”²³ – are nominal. We believe that reported costs were improperly inflated by the inclusion of fees paid to processors performing outsourced ACS services, where the processor’s profit margin is likely included in the fees, and therefore such fees should be excluded. See NPRM at 81735. Because the statute requires that allowable fees be limited to actual cost, such profits should be excluded. One way to do that is to limit allowable ACS costs to the average ACS costs for issuers that handle these functions in-house.²⁴

D. Rules Should Limit Allowable Costs to ACS (i.e., Non-Fraud) Costs

Dell supports the Board’s strict limitation of allowable costs to the issuer’s role in authorization, clearance, and settlement, in accord with the clear intent and plain text of the statute. See NPRM at 81734-35 (“This formulation includes only those costs that are specifically mentioned for consideration in the statute.”).

Under the Act, any adjustment to interchange based upon fraud prevention costs clearly belongs in a separate rulemaking under a different provision, EFTA § 920(a)(5). The Act’s plain text and statutory structure mandate separate consideration of issuer ACS costs and any “adjustments” for fraud prevention costs borne by all parties. This is confirmed by the Act’s legislative history. Senator Durbin, discussing the text of the Act on the Senate floor, stated that “It should be noted that any fraud prevention adjustment to the fee amount would occur after the base calculation of the reasonable and proportional interchange fee amount takes place, and fraud prevention costs would not be considered as part of the incremental issuer costs upon which the reasonable and proportional amount is based.”²⁵

²² See Merchant Payment Coalition Comments, *Industry Facts Concerning Debit Card Regulation Under Section 920* at 1,

http://www.federalreserve.gov/newsevents/files/merchants_payment_coalition_meeting_20101102.pdf (citing First Annapolis Consulting, “STAR CHEK® Direct Product Overview,” Prepared for First Data, June 22, 2004, at 25; First Annapolis POS Debit Issuer Cost Study Comprehensive Report, Presented to First Data and STAR, Oct. 23, 2007, at 26, 28).

²³ Complaint ¶ 94, *TCF Nat’l Bank v. Bernanke*, No. 10 Civ. 4149 (D.S.D. Oct. 12, 2010).

²⁴ In fact, because the largest providers of outsourced processing handle volumes which are comparable or greater than the largest issuers, the true ACS costs to these providers are very low.

²⁵ 156 Cong. Rec. 105, S5925 (July 15, 2010) (“Further, any fraud prevention cost adjustment would be made on an issuer-specific basis, as each issuer must individually demonstrate that it complies with the standards established by the Board, and as the adjustment would be limited to what is reasonably necessary to make allowance for fraud prevention costs incurred by that particular issuer.”).

The Board properly rejected efforts by issuers and payment networks to distort these costs, such as by importing fraud prevention through an overly broad definition of authorization. *See* NPRM at 81760 (“An issuer generally performs separate activities with the primary purpose of fraud-prevention in connection with authorization. Those separate activities are not considered to be part of an issuer’s role in authorization under § 235.3(c)(1).”).

While the Board properly rejected efforts to import customer service costs into ACS, noting for example that *inquiries* about transactions are not part of clearance costs (NPRM at 81760), allowing the costs of “non-routine transactions” such as “chargeback messag[ing]” effectively imports fraud costs into the ACS calculation. *See* NPRM at 81739. The majority of chargebacks fall under fraud reason codes for Internet merchants, and thus, including these costs imports fraud costs into the ACS calculation. Moreover, “initiating the chargeback message, and data processing and reconciliation expenses specific to receiving representments” are not part of the properly defined “clearance” function of an issuer. Most importantly, fraud-related non-routine transaction costs should be addressed as part of the separate fraud adjustment, and including those costs as part of the ACS calculation runs the risk of double counting to the detriment of merchants. For these reasons, we urge the Board to exclude chargeback costs from the ACS calculation.

IV. Fraud Adjustment

A. Fraud Must Be Defined to Include “Friendly Fraud” Authorized by the Cardholder

The EFTA provides that the Board’s fraud adjustment standards must account for merchant costs of fraud and fraud prevention. *See* EFTA § 920(a)(5)(A)(ii)(I), 920(a)(5)(B)(ii). Dell notes that the NPRM’s proposed definition of fraud – derived from the existing EFTA definition of “unauthorized electronic fund transfer” – is too limited by focusing only on theft of a card or card data. NPRM at 81740 (“[T]he Board believes 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.”).

This definition excludes a large – and growing – category of fraud known as “friendly fraud.” Friendly fraud is fraud committed *by cardholders* or other *authorized* card-users.²⁶ To the extent the definition of fraud informs the adoption of rules and the measurement of any fraud adjustment – which by statute must consider the costs of fraud

²⁶ Based on recent estimates, as much as one-third of card-not-present chargebacks for fraud are in fact the result of “friendly fraud” that cannot be attributed to the merchant. Digital Transactions News, *‘Friendly Fraud’ Grows Worse, But Chargebacks Winnable, Expert Says* (Mar. 6, 2008); Pui-Wing Tam, *Businesses Get Tougher on ‘Friendly Fraud’*, Wall St. J. (May 26, 2009) (noting 50% spike since October 2008); Digital Transactions News, *On the Rise, Friendly Fraud Is Getting Online Merchants’ Attention* (Mar. 18, 2010) (noting friendly fraud estimates of 70% for digital-goods merchants and 20% for e-commerce catalog merchants); CyberSource Online Fraud Report 2011 at 18 (62% of merchants report friendly fraud has increased with the declining economy of the last two years).

to all parties – it is vital for Internet merchants that “friendly fraud,” and the costs it imposes, be taken into account.²⁷

B. The Board Should Adopt a Technology-Based, Yet Non-Prescriptive Approach

The Board should make clear that no fraud adjustment may be provided to issuers for existing, out-moded technology based upon the magnetic stripe.²⁸ Instead, any fraud adjustment must depend upon the implementation of what the NPRM calls “paradigm-shifting” technologies. NPRM at 81742.

However, the Board need not adopt technology-specific standards. Rather, the fraud adjustment rule should establish technology-neutral eligibility standards based upon performance metrics. An issuer would be eligible for a fraud prevention adjustment – for a limited time (not to exceed five years) to recover the issuer’s capital investment – if that issuer implements a technology that both significantly reduces fraud and is cost effective.²⁹ To be eligible, issuers must submit a proposal detailing the benefits of the technology and long term effects of its implementation. Qualifying fraud prevention technology must (a) result in debit card fraud losses which are materially lower (*e.g.*, at least 10%) than industry-wide PIN debit transaction fraud losses (reported as 3.5 basis points at NPRM at 81741), and (b) incur costs which are less than the amount of fraud losses eliminated by its use (*i.e.*, the benefits exceed the costs).

Eligibility must require issuers to accept liability for all fraud (including chargebacks and fees) which occurs on qualifying technology. This liability shift is consistent with current issuer liability for PIN debit fraud, where issuers bear “nearly all” – 96% – of associated fraud. NPRM at 81741. Given the experience of card-not-present merchants – that assume the vast majority of the costs of fraud (some 76% of direct fraud losses, NPRM at 81741) and undertake substantial fraud prevention investments of their

²⁷ In its annual study of online fraud, CyberSource (now owned by Visa) reports that fraud chargebacks alone – the fraud measure used by networks and issuers – “understate fraud loss by as much as 50%”:

This year’s survey again probed the percent of fraud losses due to chargebacks. Overall, merchants continue to report that chargebacks accounted for less than half of fraud losses. The remainder occurred when merchants issued credit to reverse a charge in response to a consumer’s claim of fraudulent account use. . . . At the same time 62% of merchants say they perceive that “friendly fraud” has increased over the past two years, as unemployment has risen. CyberSource Online Fraud Report 2011 at 5.

²⁸ The Chairwoman of the House Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology concluded nearly two years ago that “[m]agnetic stripe-based technology is outmoded and inherently less secure . . . [and] the payment card industry and issuing banks should be ashamed about the current state of play and doing everything possible to immediately institute improvements in infrastructure.” Statement of Subcommittee Chairwoman Yvette D. Clarke, *Do the Payment Card Industry Data Standards Reduce Cybercrime?* (Mar. 31, 2009).

²⁹ As the Board noted, the fraud adjustment need not reimburse all issuer costs. “This approach would shift some or all of the issuers’ ongoing fraud-prevention costs to merchants, even though many merchants already bear substantial card-related fraud-prevention costs, particularly for signature debit transactions.” NPRM at 81742.

own – it is critical that issuers do not receive any positive adjustment for fraud before this liability shift is in place.

Issuer assumption of liability for fraud will provide a substantial incentive for card-not-present merchants to participate in new technology. If issuers bear as much of the cost of fraud as they claim – 57% for signature debit and 96% for PIN debit transactions – and if card payment fraud is as significant a concern for them as they claim, this approach should provide strong incentives to invest in – and recover the costs of – innovative fraud prevention techniques. NPRM at 81741.

Because this approach gives merchants and issuers adequate incentives to implement new paradigm-shifting technologies, it should also include a strict prohibition against networks or issuers forcing merchants to implement any specific technology.³⁰ Therefore, an issuer should receive reimbursement only from merchants who choose to use an eligible technology, for a limited time (no more than five years) for that issuer to recoup the initial capital investment necessary to implement a particular qualifying technology.

C. Calculation of the Fraud Adjustment Must Account for Merchant Fraud Experience

As discussed above, Internet merchants have long faced discriminatory rates of interchange supposedly based upon the higher risk of fraud associated with card-not-present transactions. The Board's fraud adjustment standards should recognize that there are scofflaws and high risk merchants in *both* the card-present and card-not-present environments. Because of the growing number of high quality, low fraud Internet merchants such as Dell, the Board should be careful to avoid standards which penalize all card-not-present transactions, especially as this is a rapidly growing sector.

For merchants – regardless of sales channel – that experience a rate of fraud lower than 1%, we propose a fraud adjustment no greater than the 1.2 cent cost per PIN debit transaction for fraud prevention identified in the NPRM. NPRM at 81741 n.75.³¹ Issuers could recover up to 1.2 cents per transaction for all transactions that use the eligible

³⁰ Merchant choice in adoption is important, especially for Internet merchants. For example, even though they have been in existence for years, Internet authentication services such as “Verified by Visa” or MasterCard’s “SecureCode” are used only on a minority of CNP transactions. The flaws in these services (which involve a disruptive customer experience because customers must leave merchant websites and return after verification, causing abandonment) coupled with weak security benefits have led to low levels of adoption. As CyberSource (now a subsidiary of Visa) recently observed, “despite significant interest in implementing payer authentication systems over the past few years, we have seen relatively slow actual adoption of payer authentication since we started tracking this tool in 2003.” CyberSource Online Fraud Report 2010 at 9. In 2011, CyberSource reported that only 16% of larger Internet merchants use either product. CyberSource Online Fraud Report 2011 at 8, chart 3 (reproduced above); see Kate Fitzgerald, *Report: 3-D Secure Not What Name Suggests*, Am. Banker (Feb. 3, 2010).

³¹ We note that this cost is significantly higher than other reports, such as a 2007 First Annapolis Consulting study which identified large issuer costs for fraud and risk management as 0.7 cents for signature debit and 0.02 cents for PIN debit. See First Annapolis Consulting, *POS Debit Issuer Cost Study Comprehensive Report* (2007) at 38.

technology, depending upon the reduction in average fraud loss per transaction. Specifically, the issuer would qualify for a prorated fraud prevention adjustment equal to 1.2 cents times the percentage by which the issuer's technology reduces its debit card fraud losses on a transaction value basis below the industry-wide debit card fraud losses as determined by the Board. For example, if debit card fraud losses are 67% lower than the norm for PIN debit transactions, then the issuer would qualify for a fraud prevention adjustment of 0.8 cents (67% of 1.2 cents).³²

High risk merchants – regardless of sales channel – who experience fraud at a rate greater than 1% would be subject to the full 1.2 cent fraud adjustment. This class of high risk merchants is already identified by the payment networks. The networks currently monitor chargeback rates and enforce a 1% chargeback threshold.³³ High risk merchants who exceed this threshold – based upon the demonstrated risk experience of individual merchants, not merchant category – are subject to additional monitoring and substantial fees and fines.³⁴

This approach distinguishes low fraud, high quality merchants from genuinely high risk merchants, regardless of sales channel. The approach is also easy to administer, as it employs existing network monitoring. Moreover, fees and fines for excessive chargebacks collected by networks adequately compensate issuers for the additional fraud introduced to the system by high risk merchants, without imposing a penalty upon low fraud merchants who undertake great expense to prevent fraud.

V. For Internet Merchants, Meaningful Limits on Network Exclusivity Must Turn on Authorization Method

Limits on network restrictions need to be sufficiently flexible to enable Internet merchants to have routing choices as new technologies develop. As the Board observes, Internet retailers have no widely available alternative technology that could cut merchant costs. See NPRM at 81723; 81741 & n.70, 81749. Because Internet transactions currently depend upon signature debit, only Alternative B (requiring two unaffiliated networks for each authorization method, including, possibly, new methods for Internet transactions) will provide any meaningful benefit to Internet merchants. We think

³² The Board may wish to take into account the disproportionate impact this adjustment could have on low dollar transactions.

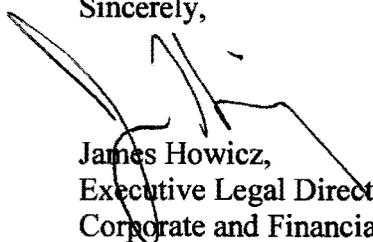
³³ See Visa International Operating Regulations (Oct. 2010) at 677, <http://corporate.visa.com/media/visa-international-operating-regulations.pdf>; MasterCard Rule 8.6.1, Excessive Chargeback Program, http://www.mastercard.com/ca/wce/PDF/Excessive_Chargeback_Guide_2009.pdf.

³⁴ For example, under current MasterCard rules, if a merchant exceeds the 1% threshold for two consecutive months, the merchant must pay an “issuer reimbursement fee” of \$25 for each chargeback over the threshold, which amount is then multiplied by the chargeback rate for a “violation assessment.” MasterCard Excessive Chargeback Program, Rule 8.6.3, http://www.mastercard.com/ca/wce/PDF/Excessive_Chargeback_Guide_2009.pdf. The following example is provided in the MasterCard rules: For a qualifying month in which a merchant had a 1301 chargebacks and a chargeback rate of 1.36%, the merchant would owe \$8,650 for issuer reimbursement and \$11,764 as an assessment, or \$20,414 total. *Id.* at 5.

Alternative B is especially important in the event the Board elects to implement the stand-alone cap alternative to § 235.3. If the Board is inclined to adopt that approach in the hope that networks will compete for volume by setting rates below the cap, that will not work – and the result will be that the cap is effectively converted into a 12 cents safe harbor – if most merchants (including all card-not-present merchants) have no routing options (which will be the case for the foreseeable future under Alternative A). Moreover, in our view Alternative B can and should be implemented by early 2012. For these reasons we support Alternative B and respectfully suggest that it could be implemented by that time.³⁵

Thank you in advance for your attention to the comments in this letter. Please let me know if you have any questions.

Sincerely,



James Howicz,
Executive Legal Director
Corporate and Financial Services

³⁵ In our view, the costs of implementation have been vastly overstated by the networks and issuers. Issuers can add networks without reissuing cards, and smaller issuers can use gateways to cost-effectively add network linkages. Nonetheless, we advocate giving the industry some additional time to make necessary adjustments.