SUBMISSION OF DELL, INC.
TO THE BOARD OF GOVERNORS
OF THE FEDERAL RESERVE SYSTEM
REGARDING SECTION 920 OF THE
ELECTRONIC FUND TRANSFER ACT

Redacted Version for Public Release

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Since the Internet became a commonly used medium for commerce in the 1990s, the payment industry has required Internet merchants to pay discriminatory interchange rates much higher than rates paid by their traditional, brick-and-mortar competitors. At the time, the justification offered was the supposedly higher fraud risks Internet merchants introduced to the system because the payment card was not physically presented for inspection in an Internet transaction. These interchange rates – known as "card not present" or "CNP" rates – are sometimes more than *double* the rate for "card present" retail transactions, costing Internet merchants millions in additional fees each year.

The inequities inherent in this system have been compounded by the fact that, in addition to paying excessive and discriminatory interchange, Internet merchants have absorbed the costs of the vast majority of the fraud associated with payment card transactions. Internet merchants, in effect, pay twice. And to make matters worse, the exorbitant interchange fees paid by CNP merchants have dissuaded networks and banks from supporting alternative technologies that could have reduced fraud and chargeback risks. This discriminatory structure has remained intact well over a decade after Internet commerce began to flourish, even though numerous sophisticated Internet merchants have managed to drastically reduce fraud through smart investments in fraud detection systems.

Against this backdrop, this White Paper advances the following broad conclusions:

- All merchants must be treated the same for ACS costs. The standards for debit interchange should eliminate the discriminatory distinction between card present and CNP merchants. Whether the standards mandate that debit transactions be interchanged at par, which we consider to be the correct result, or that interchange be limited to the true (and very low) incremental costs of authorization, clearance, and settlement ("ACS"), the result should apply equally to card present and card-not-present merchants.
- Any fraud adjustment must fully account for merchant costs. The Board should set technology-neutral standards that allow an adjustment for fraud prevention as "reasonably necessary" only when the issuer has taken "effective steps" to reduce fraud such that the issuer would be prepared to absorb all or virtually all chargeback risks after these "effective steps" have been implemented. And, consistent with the statute, no positive interchange should be allowed as a fraud adjustment unless the extensive fraud prevention, PCI, and chargeback costs of Dell and other CNP merchants have been deducted from any interchange issuers seek under this rulemaking. This calculation should also reflect the fraud that merchants eliminate from the system each year through fraud prevention efforts.

BACKGROUND

I. Dell Pioneered E-Commerce Beginning in the 1990s

Founded in 1984, Dell is now one of the largest technology companies in the world. Dell offers a range of products and services, including desktop personal computers (PCs), laptops, mobility products, software and peripherals, servers and networking, and storage, as well as IT and business related services, including infrastructure technology, consulting and applications, and business process services. For the fiscal year ending January 29, 2010, Dell generated $52.9 billion in revenue and $1.4 billion in net income. The company employs

some 37,000 people in the U.S. and 96,000 worldwide. It is the 38th largest company in the U.S.[1]

Dell launched Dell.com as a static webpage in 1994 and started selling computers on the Internet in 1996. By 1997, Dell became the first company to record $1 million in online sales.[2] Today, Dell.com reaches customers in 166 countries and 34 languages around the world. The site receives more than four million visits every day, and an online order is placed every two seconds.

Dell's PC Internet sales model was groundbreaking, as Dell was one of the first high-ticket, high-volume, hard-goods companies to conform its business model completely to the Internet. Indeed, Dell is responsible for much of the change in the way consumers perceive buying goods over the Internet. An e-commerce pioneer, the company and its business model is widely studied.[3]

Dell has paid millions in excessive interchange fees. In 2009, U.S customers placed 12 million credit and debit card orders at Dell for $5.5 billion in sales. [DELL CONFIDENTIAL & PROPRIETARY INFORMATION].[4] In 2009 alone, Dell paid [DELL CONFIDENTIAL & PROPRIETARY

---

[1] Fortune 500 (May 3, 2010), available at http://money.cnn.com/magazines/fortune/fortune500/2010/states/TX.html.

[2] James Maguire, *Case Study: Dell.com*, ecommerce-guide.com (Mar. 3, 2003), http://www.ecommerce-guide.com/news/trends/article.php/10417_2013731.

[3] An Internet search for *Dell e-commerce case study* generates hundreds of thousands of results. *See, e.g.*, Maguire, *Case Study: Dell.com* (quoting Forrester analyst discussing the "second wave" of Internet commerce, where consumers "start with low-ticket, low-risk goods like books, and they eventually begin to trust the Internet more and graduate to higher end products like PCs and travel").

[4] This example compares Dell's actual interchange paid, not including acquirer fees, in 2009, using the same the transaction data with interchange at Visa's CPS Retail Threshold 1 rate, or 0.62% and $.13 per transaction. *See* Appendix 1; *Visa U.S.A. Interchange Reimbursement Fees* at 2, http://usa.visa.com/download/merchants/october-2010-visa-usa-interchange-rate-sheet.pdf.

INFORMATION] more in interchange fees than a comparable brick-and-mortar merchant would have paid over the same period.

II. The Current System Discriminates Against Internet Merchants

The current payment system discriminates against Internet and other so-called CNP merchants in several important ways. First and foremost, Internet merchants pay substantially higher interchange rates for all transactions (debit or credit) than their competitors in traditional brick-and-mortar categories.

Second, Internet merchants receive virtually no protection against chargebacks.[5] Instead, Internet merchants bear the vast majority of the fraud risk on transactions made on their sites. This risk is compounded by network zero liability policies and chargeback thresholds.

On top of all this are chargeback thresholds which require merchants to keep chargeback ratios below 1% of their total Visa and MasterCard volumes.[6] As a result, to avoid exceeding the thresholds, Internet merchants adopt screening procedures which have the inevitable effect of turning away legitimate transactions.[7]

The Act dictates that the Board broadly consider "the nature, type, and occurrence of fraud" in debit transactions, EFTA § 920(a)(5)(B)(ii)(I), and

---

[5] Chargebacks result when customers ask their bank to remove a charge from their payment card account. This may occur when customers state they did not receive an item or there was a problem with the item they received. Chargebacks also occur when a customer claims their card – or account information – was stolen and used by a thief to make a purchase. With each chargeback, the issuer submits a numeric "reason code."

[6] Additional reporting under MasterCard's chargeback monitoring program is triggered by a chargeback ratio above 0.5%. *See* MasterCard Rule 8.6.1, Excessive Chargeback Program, http://www.mastercard.com/ca/wce/PDF/Excessive_Chargeback_Guide_2009.pdf.

[7] Internet merchants reject 2.4% of orders. CyberSource Online Fraud Report 2010 at 15-16. Visa acquired CyberSource earlier this year.

account for the liability of all parties for fraud loss and fraud prevention costs, EFTA § 920(a)(5)(B)(ii)(IV &V). 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.

A. Internet Merchants Pay Substantially Higher Interchange Rates

Interchange fees are significantly higher for CNP transactions than for transactions in other merchant categories where the card and the merchant are physically present. Higher interchange rates apply even for multi-channel merchants selling the same goods with the same risk management system. Overall, for signature (non-PIN) debit card transactions, current Visa and MasterCard interchange rates are roughly 65 basis points higher for Internet merchants.[8] This means that over the last year, based on a conservative estimate of the overall e-commerce market, Internet merchants paid a debit interchange penalty of some $530.4 million over what they would have paid as brick-and-mortar retailers.[9]

---

[8] A table of debit interchange rates from 2001-2010 is attached as Appendix 1.

[9] This estimate is based upon an interchange premium of 65bps applied to 30% (to reflect debit card usage) of (a) the non-travel online market, calculated by the Census Department to be approximately $160 billion, *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; and (b) the online travel market, at $112 billion, *see PhoCusWright's U.S. Online Travel Overview Eighth Edition*; *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). This number is conservative in that it does not include two very substantial Internet markets: digital downloads and small business purchases. Although debit cards account for 65% of all sales in the first half of 2010, *see* Alexis Leondis, *Cardholders Prefer Debit as Credit-Card Use Falls* (Sept. 8, 2010) (citing the Nilson Report), *http://www.bloomberg.com/news/2010-09-08/cardholders-prefer-debit-as-credit-card-use-falls-*

The increased rate for CNP transactions was originally justified because of higher operational costs associated with handling customer disputes on potentially fraudulent CNP transactions. These rates were established in the late 1990s, when the Internet was in its infancy and much of the fraud prevention techniques used by Dell and others had yet to be tested or deployed. Since that time, sophisticated Internet merchants developed the business of e-commerce and designed highly effective fraud prevention and risk management systems. By late 2003, it was already obvious that the higher rates, coupled with the shift of fraud liability and risk management responsibilities to Internet merchants, had created indefensible inequities in the system.[10] Yet, since then the system has become more discriminatory for these merchants.[11]

B. Internet Merchants Absorb the Vast Majority of Chargebacks

In addition to paying higher interchange rates, Internet merchants absorb a disproportionate share of all payment card fraud losses, including direct fraud,

---

javelin-says.html, on the Internet debit accounts for 30% of payments. *See* emarketer.com, *US Online Research Payment Volume Share, by Payment Method, 2007-2013 (% of total)*.

[10] Mark Betz, *Chargebacks and Consumer Behavior*, Transaction World (Oct. 2003), http://www.transactionworld.net/articles/2003/october/coverstory.asp. It is worth noting the common perception in the industry in the late 1990s that, because of the security limitations of magnetic stripe payment cards, many consumers were unwilling to use their cards over the Internet to make purchases. *See, e.g.*, Helen K. Simon, *The E-tailer's Dilemma*, Vol. 8, Issue 2, J. Applied Mgmt. & Entrepreneurship 75, 2003 WLNR 17717033 (Apr. 1, 2003) (discussing research into consumer fears of Internet commerce in the late 1990s). That has changed dramatically over the years. "Today, 63% of consumers indicate that they are comfortable or very comfortable with shopping online . . . ." Jack Loechner, *Consumers Comfortable Shopping Online with Credit Cards* (Mar. 10, 2010) (citing Javelin Strategy and Research), http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=123814. This increased confidence should be attributed, in part, to the success of merchants such as Dell in policing fraud.

[11] *See* Appendix 1 (showing that the differential between card-present and card-not-present rates has increased over time such that current rates are more than double those available to high-volume brick-and-mortar merchants); *Visa U.S.A. Interchange Reimbursement Fees* at 2, http://usa.visa.com/download/merchants/october-2010-visa-usa-interchange-rate-sheet.pdf (compare CPS Retail - Threshold 1, at CPS/Retail Debit—Performance Threshold1 I, at 0.62% + $0.13 per transaction, with CNP 1.60% + $0.15 per transaction).

escalating fraud management costs, and lost sales turned away to avoid chargeback thresholds. Under the current system, Internet merchants absorb the bulk of the cost of fraud through chargeback rules and policies imposed by the payment card brands. Because of these network rules, Richard Sullivan, a Senior Economist at the Federal Reserve Bank of Kansas City, concluded 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 CNP transactions."[12]

Chargeback rules allow merchants to re-present a chargeback if they can produce a signature and verify that they complied with the rules at the point-of-sale. The rules were not designed to accommodate the different indicia that Internet merchants collect to authenticate a cardholder. As a result, in practice Internet merchants have limited ability to contest chargebacks, in contrast to brick-and-mortar merchants.[13] Industry-wide, Internet merchants pay for 80% of all chargebacks. On top of this, they absorb the costs of the goods, shipping, and charge-back research and re-presentment fees.[14] [DELL CONFIDENTIAL & PROPRIETARY INFORMATION]

Merchants are also charged fees for every chargeback they re-present, and may pay additional fees if the chargeback is not reversed upon re-presentment.

---

[12] 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 111 (2d Qtr. 2010), http://www.kansascityfed.org/Publicat/Econrev/pdf/10q2Sullivan.pdf.

[13] Depending on the circumstance, Internet merchants may succeed in re-presenting chargebacks. For example, if a merchant has a signed delivery receipt, or has accumulated evidence such as address verification (AVS) and card verification number (CVN), it may successfully re-present the charge. The merchant pays for this right of presentment in related fees.

[14] *See* Jane Adler, *Checking the Chargeback Scourge*, Digital Transactions at 36 (chart), 38 (June 2010), http://www.digitaltransactions.net/files/DigitalTransactionsJune2010.pdf.

Chargeback fees have been increasing and in some cases (e.g., for small Internet merchants) fees may exceed the value of the transaction.[15] The inequities of the system are compounded by the chargeback threshold of 1% of total volume that Visa and MasterCard require Internet merchants meet.[16] Exceeding this threshold triggers onerous fees and fines.[17] While Dell's chargeback ratio is well below the threshold, many Internet merchants must turn away substantial numbers of legitimate transactions with overly tight constraints on suspect orders. In addition, merchants typically offer credits to customers who complain of fraud to avoid chargebacks. As a result, chargebacks alone understate losses due to fraud-related issues by as much as 50%.[18]

[DELL CONFIDENTIAL & PROPRIETARY INFORMATION][19] This rate is comparable to that of many brick-and-mortar merchants.[20] This is

---

[15] A First Annapolis acquirer survey found that the percentage of acquirers that charge chargeback fees in excess of $20 tripled between 2001 and 2007. Charles Marc Abbey, *The Threat to Price Stability in the Small Merchant Market*, Digital Transactions at 16 (June 2008), http://www.digitaltransactions.net/files/0608acq.doc.

[16] *See* Visa International Operating Regulations at 703, http://usa.visa.com/download/merchants/visa-international-operating-regulations-main.pdf; MasterCard Rule 8.6.1, Excessive Chargeback Program, http://www.mastercard.com/ca/wce/PDF/Excessive_Chargeback_Guide_2009.pdf.

[17] For example, under 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.

[18] *See* CyberSource Online Fraud Report 2010 at 5, 19 ("Revenue loss measurement includes not only the value of orders on which fraudulent chargebacks are received, but also the cost of any credits issued to avoid such chargebacks.").

[19] [DELL CONFIDENTIAL & PROPRIETARY INFORMATION] "Friendly fraud" has developed under network rules providing "zero liability" for cardholders. It refers to fraud by a cardholder who repudiates a legitimate transaction that he/she or family member actually made. Friendly fraud is estimated to account for one third of all chargebacks for Internet purchases. Digital Transactions News, *'Friendly Fraud' Grows Worse, But Chargebacks Winnable, Expert*

particularly low for a consumer electronics company, as these merchants are often targets of fraud.[21]

Dell's success is a result of its highly effective fraud prevention systems, which are discussed below. [DELL CONFIDENTIAL & PROPRIETARY INFORMATION]

1. Internet Merchants Employ a Number of Sophisticated and Expensive Techniques to Police Fraud

Dell's success in reducing fraud is the result of substantial investments in anti-fraud techniques. [DELL CONFIDENTIAL & PROPRIETARY INFORMATION][22] Over the same three year period, Dell stopped over [DELL CONFIDENTIAL & PROPRIETARY INFORMATION] in fraudulent transactions which had received authorization from issuers.[23]

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).

[20] *See* Merchant Risk Council, Press Release, *Online Fraud Rates Approaching Fraud Rates at Card-Present Retail According to 5th Annual Survey by Merchant Risk Council* (Apr. 18, 2006), https://www.merchantriskcouncil.org/index.cfm?fuseaction=feature.showFeature&FeatureID=75&varuniqueuserid=07845376812 ("Card-present fraudulent chargeback rates are usually less than 0.1% of sales. 48% of the online retailers surveyed said that their chargebacks match that rate, a significant improvement over previous years when online fraud outpaced card present fraud by as much as five times.").

[21] *See* CyberSource Online Fraud Report 2010 at 21 ("Consumer Electronics reported the highest fraudulent [accepted] order rate, averaging 1.5%, but this was down from 2.0% in 2008."). Overall, the fraudulent accepted order rate in the industry is approximately 0.9%. Cyber Source Online Fraud Report 2010 at 4, 16-17.

[22] 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* note 9, above.

[23] [DELL CONFIDENTIAL & PROPRIETARY INFORMATION]

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 checks to determine the risk of a given transaction, and typically separate out up to 25% of those transactions for additional, manual review.[24]

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.[25]

- Data Collection. A sophisticated Internet merchant deploys an elaborate platform for accessing databases where transaction data is collected and assimilated. In addition to basic order and payment information, Internet merchants collect information about an individual transaction session, including IP address, ISP, and increasingly, device ID information.
- Business Rules. This 'raw' information is processed by a variety of fluid business rules to associate the data with prior history of customer activities, including prior fraud or chargebacks. [DELL CONFIDENTIAL & PROPRIETARY INFORMATION] including various velocity checks that spot suspicious transactions based on purchasing patterns, including purchasing frequency. PCI DSS rules, however, reduce merchants' screening ability by prohibiting storage of card information unless it is tokenized or encrypted.[26] Internet merchants also use transaction

[24] CyberSource Online Fraud Report 2010 at 11.

[25] 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.

[26] As discussed below in Section II.C, the PCI Council, owned by the five payment networks, sets mandatory standards concerning the security of payment data, and requires that certain cardholder data may not be stored. *See* PCI-DSS Guidance for Requirement 3.1 ("Extended storage of cardholder data that exceeds business need creates an unnecessary risk. The only cardholder data that may be stored is the primary account number or PAN (rendered unreadable), expiry date,

"scoring," which they sometimes outsource to providers who have modeled accumulated experience into neural networks "trained" on large data sets to detect patterns of negative experience.

- Manual Review. Much of the processing chain is built around manual review of suspicious transactions flagged by automated fraud detection systems.[27] Manual review is costly and labor-intensive, consuming over half of fraud management budgets.[28] Industry-wide, about 1 in 4 orders enters manual review.[29] Because of increased automation, large Internet merchants typically review 15% of orders. [DELL CONFIDENTIAL & PROPRIETARY INFORMATION]

As discussed below, this backdrop belies the issuers' claim that interchange should reflect fraud prevention costs, either as part of ACS costs or in the fraud prevention adjustment.

2. Lost Transactions Due to Fraud Prevention Measures

In addition to the cost of fraud prevention measures, Internet merchants also decline to accept a significant share of valid incoming orders due to suspicion of payment fraud. CyberSource, for example, reports that Internet merchants reject 2.4% of orders due to suspicion of fraud in 2009, down from 4.2% in 2007.[30] Valid orders are sometimes rejected because the fraud detection process attempts to balance the risk of false positives versus false negatives in examining potentially fraudulent orders to maintain chargebacks below the 1% threshold.

---

name, and service code."), https://www.pcisecuritystandards.org/pdfs/navigating_pci_dss_v1-1.pdf.

[27] Generally issuers do not perform manual review, instead simply declining the transaction and referring it as potentially fraudulent.

[28] CyberSource Online Fraud Report 2010 at 22, citing previous 4 years.

[29] *Id.* at 5.

[30] *Id.* at 15-16. CyberSource reported that consumer electronics merchants rejected 6.6% of orders in 2009. *Id.* at 16, chart 12.

3. Customer Service Costs

In addition to costs throughout the order processing chain, fraud detection also entails substantial customer service costs.

For example, when a transaction is erroneously flagged as suspicious – which, as noted, sometimes occurs when an Internet merchant is excessively vigilant to avoid chargeback thresholds – the customer usually calls the merchant's customer service center. When delays result from manual review, customers may also contact customer service about order status and/or cancel their orders and shop elsewhere. In addition, merchants incur customer service costs to address each chargeback. As a result, Internet merchants tend to incur higher customer service costs for fraud than brick-and-mortar merchants.

4. Fraud Detection Efforts Are Often Proprietary and Are Not Shared Among Merchants

As sophisticated Internet merchants have developed increasingly effective techniques to protect against fraud, they have had little interest in sharing this expertise with the industry, given the competitive advantage they obtain from these systems. In this regard, keeping this information proprietary avoids dilution and the risk the strategies will be exposed to wider challenge and defeated.

This highlights the problems inherent in a system that puts the burden on merchants as opposed to issuers, who are much better positioned to police fraud. Issuers choose the authentication technology used on their cards, make risk-based underwriting decisions, collect and accumulate information about card use, history, spending behaviors, locations, and products purchased, across all merchants, which can be aggregated and analyzed to detect suspicious

transactions. Individual merchants, on the other hand, can only screen fraud from a single transaction in a single session. As such, even with the sophisticated tools that Dell and other Internet merchants bring to bear, the issuers are still in the best position to catch fraud. That issuers, who claim to use fraud prevention as an add-on to the authorization process, nonetheless authorize millions in fraudulent transactions that are later caught by Dell and other Internet merchants reflects the fact that the current system does not provide issuers sufficient incentives to police fraud.

C. PCI Compliance Costs Are Substantial and Compliance Does Not Prevent Liability in the Event of Breach

PCI DSS imposes stringent data security requirements on merchants as well as other participants in the payments system. As Richard Sullivan notes, implementing PCI DSS has been controversial, and merchants and processors especially face significant compliance costs and question the benefits they receive.[31] Development of the standard has been perceived as one-sided, favoring issuers over merchants.[32]

PCI compliance requires a variety of ongoing expenditures – from establishing a vulnerability management program to performing regular monitoring and assessment of all systems. Annual auditing and recertification is

---

[31] Sullivan, *Changing Nature of U.S. Card Payment Fraud* at 119.

[32] *Id.* at 121. *See also* SmartCards Trends (June 10, 2009) (reporting joint letter from merchant groups advocating more transparency and collaboration in the development of data security standards), http://www.smartcardstrends.com/det_atc.php?idu=9557. Founded in 2006, the PCI Council is owned by the five global payment brands – American Express, Discover, JCB International, MasterCard, and Visa. Representatives from the five brands make up the PCI Council's policy-making Executive Committee as well as the Management Committee. While some of the PCI Council's 500 members are merchants who may vote for representatives to the Board of Advisors, merchants have little influence in the design and implementation of PCI standards.

also required, which imposes additional costs. But even if a merchant has been deemed fully compliant, if a breach occurs on the merchant's systems, the merchant is automatically deemed non-compliant. The merchant must pay all card reissuance costs, as well as bear liability for any perceived (as opposed to actual) increase in fraud in the area of the breach, even if the fraud cannot be attributed to the breach.[33] Merchants are assessed penalties based on the difference between the "normal" rate of fraud and any additional fraud in the area that the networks contend, without proof, was caused by the breach. As has happened in several recent breaches involving merchants, it makes no difference that the merchant was using software and following procedures deemed PCI DSS compliant. When a breach happens, the merchant is automatically found guilty and assessed punitive fees and fines.

III. The Current System Discourages the Use of Superior Technology with Lower Risk of Fraud

The flawed incentives created by the current system are readily apparent. As Richard Sullivan observed, although other countries suffer lower rates of fraud than the U.S., these countries have been motivated to make major technological steps to adopt cards that move away from the magnetic stripe. In contrast, in the U.S., substantially higher rates of fraud have not led to same motivation, whether for smart cards or some other comprehensive and coordinated solution.[34]

---

[33] Visa, *Updated Account Data Compromise Recovery (ADCR) Frequently Asked Questions* at 6 (Mar. 19, 2008), http://www.rbsworldpay.us/247/pci_docs/ADCR_FAQs.pdf.

[34] Sullivan, *Changing Nature of U.S. Card Payment Fraud* at 121; *see also* Richard J. Sullivan, *Can Smart Cards Reduce Payments Fraud and Identity Theft?*, Federal Reserve Bank of Kansas City, Economic Review (3d Qtr. 2008), http://www.kansascityfed.org/PUBLICAT/ECONREV/PDF/3q08Sullivan.pdf. The Act directs the Board to consider the occurrence of fraud in signature versus PIN debit, EFTA

For example, after nearly a decade, PIN debit transactions – which clear faster, are less vulnerable to fraud, and incur lower interchange rates – are almost completely unavailable to Internet merchants.[35] Products that could facilitate PIN debit purchases over the Internet have been available for the better part of a decade, but have not gained traction.[36]

At the same time, 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, and only when the merchant and issuer both participate in the service. 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

---

§ 920(a)(5)(B)(ii)(II), as well as "available and economical means" for reducing debit fraud, EFTA § 920(a)(5)(B)(ii)(III). The Act also directs the Board to consider past incentives or lack of incentives to reduce fraud under the existing interchange system. EFTA § 920(a)(5)(B)(ii)(VI).

[35] Digital Transactions, *Web Merchants Set High Hurdles for Alternative Payments to Clear* (Apr. 13, 2005), http://www.digitaltransactions.net/index.php/news/story/554; Lauri Giesen, *Pinned Down*, Digital Transactions 34 (May 2008), http://www.digitaltransactions.net/archivemag.cfm, http://www.digitaltransactions.net/files/0508cover.doc.

[36] Issuers have historically pushed signature debit over PIN. *See* Barbara Pacheco & Richard Sullivan, *Interchange Fees in Credit and Debit Card Markets: What Role for Public Authorities?* Federal Reserve Bank of Kansas City, Economic Review 99 (1st Qtr. 2006), http://www.kansascityfed.org/PUBLICAT/ECONREV/PDF/1q06pach.pdf; *see* 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 ("Despite all this, signature debit cards dominate debit use in this country, accounting for 61 percent of all such transactions, even though PIN debit cards are less expensive and less vulnerable to fraud.")

have seen relatively slow actual adoption of payer authentication since we started tracking this tool in 2003."[37]

ARGUMENT

I. Brick-and-Mortar and Internet Merchants Should Pay the Same – If Any – Interchange

A. Interchange Is Not Necessary, "Reasonable and Proportional"

Under the Act, interchange must be both "reasonable" and "proportional." EFTA § 920(A)(2). To be "reasonable," interchange must be *necessary*. Interchange is merely a subsidy from merchants to issuers that cannot be justified unless it is absolutely necessary because issuers would stop issuance without it. In fact, issuers would almost certainly continue to issue debit cards even without interchange because debit cards are the key access device to the core demand deposit account relationship.[38]

The Act invites the Board to consider the fact that checks clear at par in setting standards for debit. The fact that issuers have long issued checks which clear at par in order to give customers convenient access to their money reinforces the conclusion that they would do the same with more efficient electronic debit

---

[37] CyberSource 2010 at 9 & chart 3 (showing only 16% of larger Internet merchants use either product); *see* Kate Fitzgerald, *Report: 3-D Secure Not What Name Suggests*, Am. Banker (Feb. 3, 2010).

[38] In support of its November 4, 2010 motion for a preliminary injunction, TCF Bank stated that it would continue to issue debit cards because "no bank in this country could sell a checking account without a debit card feature." TCF Mem. in Support of Prelim. Injunction, Docket No. 16 at 4, *TCF Nat'l Bank v. Bernanke*, No. 10 Civ. 4149 (D.S.D. Nov. 4, 2010). In its complaint, TCF concedes that it would continue to issue debit cards after the regulations go into effect because of their importance as the key access device to the demand deposit account relationship. Complaint ¶ 7, *TCF Nat'l Bank v. Bernanke*, No. 10 Civ. 4149 (D.S.D. Oct. 12, 2010); *see also* Commerce Bank Presentation to Federal Reserve Board at 2 (Oct. 27, 2010) ("Debit Cards are now a fundamental part of retail banking. We must offer debit cards if we are to meet our customers' needs."), http://www.federalreserve.gov/newsevents/files/commerce_meeting_102710.pdf.

transactions. As demonstrated by experiences around the world, including Canada, debit issuance thrives without interchange.[39] In Canada, notably, the Interac debit network is now facilitating Internet transactions without interchange.

The conclusion that interchange is not necessary is reinforced by the experience of CNP merchants. For Internet merchants interchange is merely an exercise of market power by the networks, particularly Visa and MasterCard.[40] The networks price discriminate against Internet merchants because networks face less competition in that space and thus have greater pricing power over Internet merchants. That they compound this price discrimination by charging the Internet merchant at least twice for fraud – first with interchange, then with chargebacks – further exposes the market power that lies behind the current system.

Accordingly, under any fair reading of "reasonable and proportional" to cost, debit interchange should be at par, and that result should apply to all merchants.

---

[39] Even Visa, in its November 8, 2010 submission to the Board, could not bring itself to predict that debit card issuance would decline if interchange were reduced significantly. The best Visa could offer is that if DDA fees do not increase with lower interchange – and elsewhere it predicts that they will increase – "some electronic debit card transactions may not be offered by some institutions." In addition to declining to say that "cards" will not be issued at lower interchange, Visa does not say which "transactions" will not be offered, nor which institutions "may" stop offering them. This speaks volumes about the importance of debit to the DDA relationship. Visa's tepid and carefully worded prediction is an acknowledgment that any claim that issuers would not provide this service unless they receive interchange subsidies from merchants is simply not credible.

[40] *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* 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.

B. In the Alternative, Interchange Must Be Limited to the Very Low Incremental Cost of Authorization, Clearance, and Settlement, Which Is the Same for All Merchants

If the Board concludes that some form of positive interchange is "reasonable," it must then establish standards to ensure that the rates are set "proportional" to issuer costs. EFTA § 920(a)(2). The statute is explicit on what costs can and cannot be considered, mandating that only "the incremental cost incurred by an issuer for the role of the issuer in the authorization, clearance, or settlement of a particular electronic debit transaction shall be considered," and prohibiting consideration of any "other costs" which are "not specific to a particular electronic debit transaction . . . ." EFTA § 920(a)(4)(B)(i & ii).

As such, only incremental costs – those incurred with respect to the marginal debit transaction – may be considered. Fixed, average, lifetime, indirect, or amortized costs should not be considered. Consideration of any costs that do not meet these statutory requirements would be inappropriate.

1. Authorization Should Be Limited to Its True Definition: Verifying the Availability of Funds

ACS costs should be limited to the incremental processing costs associated with authorizing the transaction, i.e., verifying that the cardholder has sufficient funds to complete the purchase, clearing the transaction, i.e., delivering final transaction data issuers can post to the cardholder's account, and settling the transaction, i.e., calculating the final net financial position of issuers and acquirers. ACS costs are flat transaction costs that do not vary by merchant type, and thus, even if positive interchange is permitted up to ACS, the distinction between card present and CNP merchants should be eliminated.

Issuers may attempt to expand the meaning of the term "authorization" to include separate and distinct fraud prevention costs. These arguments should fail for the following reasons.

First, any adjustment to interchange based upon fraud prevention costs – which, as discussed below, would be ill-advised – 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."[41]

Second, the term authorization should be given its commonly accepted meaning – confirming the availability of funds – and nothing more. The meaning of the term authorization as distinct from fraud prevention is apparent from the description of "authorization" on the Visa Debit Processing Service (DPS) website.[42] Visa defines "stand-alone authorization" to include decisioning based on "activity limits and account balances" – the basic criteria to verify the

[41] 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.").

[42] *See* Visa Debit Processing Service, Transaction Processing, Authorization Processing, at http://www.visadps.com/services/authorization_processing.html.

availability of funds.[43] Various fraud prevention schemes are sold as additional tools that issuers may select. Visa DPS, for example, includes a number of customizable fraud systems which – at the issuer's option – may be accessed during authorization processing.[44] This reinforces the conclusion that the Act, specifically and purposefully, limited "authorization" to its core function – checking the availability of funds – and not fraud prevention.

Moreover, if there were any doubt about what the term "authorization" means, the neighboring statutory terms, "clearance" and "settlement," reinforce the traditional definition. TCF Bank, in its complaint seeking to overturn the Act, calls these the "three least expensive steps in the debit service."[45] They are narrow concepts which should be limited to processing costs associated with facilitating the completion of a particular transaction.[46]

Indeed, the terms "authorization, clearance, and settlement" have an established meaning in the payments system. In a 1997 study, *Payments, Clearance, and Settlement: A Guide to the Systems, Risks, and Issues*, the General Accounting Office wrote that:

> The clearance and settlement of credit card transactions involve three parts – authorization, clearance, and settlement. Authorization is the process by which the issuer of a credit card (card-issuing bank) approves (or declines) a transaction at the point of sale. Clearance is the process by which a credit card company collects data about a transaction from a bank (referred to as an

---

[43] Authorization Processing Product Profile at 2, http://www.visadps.com/downloads/authorization_processing_product_profile_1107.pdf.

[44] Visa DPS website, http://www.visadps.com/services/authorization_processing.html.

[45] Complaint ¶ 94, *TCF Nat'l Bank v. Bernanke*, No. 10 Civ. 4149 (D.S.D. Oct. 12, 2010).

[46] Visa's description of DPS "Settlement Services" shows no relationship to fraud prevention. *See* *http://visadps.com/services/settlement_services.html?it=l2|/services/authorization_processing.html|Settlement%20Services*.

> acquirer or the merchant's bank) and delivers the data to the card-issuing bank, which will use the information to post the transaction to the cardholder's account. Settlement is the process by which a credit card company collects funds from the card-issuing bank and pays funds to the merchant's bank for the cleared transactions.[47]

During authorization, "[t]he card-issuing bank then approves or declines the transaction based on the cardholder's account status, and the approval or disapproval is transmitted electronically to the store through the credit card company."[48] Thus, the term "authorization" should not be considered in isolation apart from the full phrase, "authorization, clearance, or settlement" found in EFTA § 920(a)(4)(B)(i), and it clearly should be limited to confirming the availability of funding.[49] That issuers authorize tens of millions of potentially fraudulent transactions, which are then caught by Dell and other Internet merchants, reinforces the conclusion that fraud costs should not be counted as part of ACS costs.

2. ACS Costs Are Substantially the Same Regardless of Merchant Type

These well-established ACS functions are virtually the same for all debit transactions, so-called CNP or card-present. Visa, for example, in its Debit Processing System material, does not offer any separate set of services for "card

---

[47] U.S. GAO, *Payments, Clearance, and Settlement: A Guide to the Systems, Risks, and Issues* at 109 (June 1997) http://www.gao.gov/archive/1997/gg97073.pdf.

[48] *Id.* at 112 (emphasis added).

[49] It is well-settled that the meaning of a word in a statute should be "known by the company it keeps." *Babbitt v. Sweet Home Chapter of Cmtys. for a Great Or.*, 515 U.S. 687, 694 (1995) (citing the canon of statutory construction, *noscitur a sociis* and *Neal v. Clark*, 95 U.S. 704, 708-09 (1878)).

not present" transactions.[50] The identity of the transaction flow for card present and card not present can be seen in a 2003 publication of the Federal Reserve Bank of Kansas City which presents several flowcharts, reproduced in Appendix 2, setting forth the well-established steps of "authorization," "processing" and "settlement."[51] 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.

Based upon their submissions to the Board, networks and issuers have apparently exaggerated any potential difference, no matter how slight, between card-present and CNP transactions to justify maintaining higher interchange rates for CNP transactions. A presentation by Visa, in particular, purports to identify several differences in the "processing environment" for Internet merchants as opposed to brick-and-mortar.[52] The notion that slight variations in processing environment for the millions of Internet transactions justifies a higher positive interchange for CNP transactions cannot withstand scrutiny.

---

[50] Very slight variations may be found in "Fraud Prevention Programs." Visa offers POS merchants "Cardholder Verification Value (CVV)" – "a unique three-digit code on the magnetic stripe of all cards to detect counterfeit or re-encoded cards" versus "Cardholder Verification Value 2 (CVV2)" which is "a unique value, printed on the reverse side of the card, to reduce fraudulent card-not-present transactions." http://visadps.com/services/authorization_processing.html. Visa also offers "Address Verification Service (AVS)" which can "confirm a cardholder's billing address to prevent fraud in the card-not-present environment." *Id.* These are the *only* card-not-present distinctions identified on the Visa Debit Processing System website.

[51] Terri Bradford et al., *Nonbanks in the Payments System*, 24-26 (Nov. 2003). Notably, the fourth "authorization" step involves authorizing "a certain amount of money" and providing an authorization code.

[52] Visa, *Presentation to the Federal Reserve on Debit Card Regulation* at 12 (July 23, 2010), http://www.federalreserve.gov/newsevents/files/visa_20100723.pdf.

Visa tries to justify higher interchange for CNP transactions by pointing to the following issues: 1) partial shipments; 2) additional merchant data collection; 3) verification services; and 4) customer service calls. We address each in turn.

Split shipments. A relatively small minority of CNP transactions cannot be fulfilled in one transaction. These orders are split based on the availability of inventory, which may generate partial reversals and separate authorizations. However, Internet merchants already pay for these exception items and thus it would make no sense to add these costs into the ACS calculation. Moreover, even if these costs were added, they would be de minimus.

Merchant Data Collection. According to Visa, CNP transactions supposedly involve the collection of additional data such as specific merchant contact information for inclusion on a cardholder's statement to help identify the transaction and facilitate cardholder inquiry. *See* Visa presentation at 12 (listing "Merchant 800 number, URL or Email address," and "Merchant data on cardholder statement" as eCommerce differences). This additional data capture – if indeed it is specific to Internet merchants – is trivial, however, and is most likely part of existing transaction messaging for card-present transactions.[53] This hardly supports maintaining the distinction between CNP and brick-and-mortar merchants.

Verification Services. Visa fares no better with its suggestion that services such as checking address verification (AVS) or card verification number (CVV2) somehow justifies additional interchange. Merchants often pay for AVS

[53] For example, ISO 8583, entitled "Financial transaction card originated messages — Interchange message specifications," sets the standards – including required fields and data elements – for systems that exchange electronic transactions made by cardholders using payment cards.

separately, and should not have to pay twice for these services to the extent they occur alongside the ACS process.[54] Moreover, these are fraud prevention costs that should not be included in the ACS calculation.[55]

Customer Service Calls. Visa lists "[i]ncreased customer service calls" as a difference for issuers processing Internet transactions. Presumably this is a veiled reference to costs associated with chargebacks, some of which begin as calls from cardholders to the issuer. These costs should not be counted as ACS costs for three fundamental reasons. First, these costs are not part of the ACS process. Second, customer service costs are largely fixed costs and separating out the incremental portion of those costs would be difficult. Third, because some of these customer service costs must relate to fraud, these costs are merely a way to improperly introduce fraud-related costs into the ACS calculation.

In considering this issue, the Board should bear in mind that the notion that chargebacks justify higher interchange for Internet merchants is particularly problematic from a policy perspective, given that issuers and the payment networks have configured the current system to impose virtually all liability for chargebacks and related fees upon CNP merchants. Given that the Act requires that these costs be considered only in the fraud adjustment rulemaking, and that CNP merchant chargeback costs likely exceed these "customer service costs," Visa's argument should be disregarded.

---

[54] *See, e.g.*, MerchantCouncil.org, Merchant Account Fees & Pricing Structures, http://www.merchantcouncil.org/merchant-account-information/rates-fees.php (citing "AVS fee"); First National Bank of Omaha Merchant Services, http://www.merchantservices.com/merchant_accounts.html (citing industry standard of $.05-.10 per transaction).

[55] *See* EFTA §§ 920(a)(4)(B)(i & ii), 920(a)(5).

3. The Act Clearly Does Not Allow Interchange Fees for All Issuer Costs Related to Debit Transactions

In its November 8, 2010 submission to the Board (the "Visa Letter"), Visa effectively concedes that the incremental costs of ACS – in Visa's words, "the computer and telecommunications processing cost of the next electronic debit card transaction handled by an issuer enjoying significant economies of scale" – are nominal.[56] Recognizing that such costs are nominal and much the same across all merchants for the vast majority of transactions, Visa argues instead that "the Board has the discretion under the statute to consider issuer costs other than incremental costs for authorization, clearing and settlement narrowly defined, so long as those costs are specific to debit card transactions . . . ."[57] Visa then asserts that virtually all issuer costs – including fixed costs – can be attributed to specific debit card transactions.[58] Visa justifies this extreme position by first ignoring the Act and then by distorting the meaning of costs "specific to debit card transactions" – a phrase not found in, and contrary to the Act – to cover virtually all costs.[59]

---

[56] Letter from Visa to Federal Reserve Board (Nov. 8, 2010), http://www.federalreserve.gov/newsevents/files/visa_comment_letter_20101108.pdf.

[57] Visa Letter at 9.

[58] Visa Letter at 14.

[59] A substantially similar letter, using much of the same language, was submitted by Oliver Ireland of Morrison Foerster on behalf of "a number of institutions" which are not identified. 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. That these institutions were unwilling to put their names to this position only reinforces how extreme it is.

For starters, the Act is not at all ambiguous about the costs that can and cannot be considered.[60] Contrary to Visa's argument that the statute is not "all inclusive," the Act sets forth expressly which costs should be "distinguish[ed]" and which costs shall and shall not be considered.[61] When the Act does address another category of costs other than ACS costs which relate to an issuer's overall debit transactions – fraud costs – it does so in a completely separate provision. EFTA § 920(a)(5). Thus, the Act's text and its structure is clearly "all inclusive" as to what Congress intended may be recovered as part of debit interchange fees.

The use of the term "particular" in the Act reinforces the conclusion that Congress expressly intended that the costs in question be limited to transaction-specific incremental ACS costs. Tellingly, throughout this portion of the Act, the term "transaction" is used in its singular, not plural, form. The statute gives the Board regulatory power over "any interchange transaction fee that an issuer may receive or charge with respect to *an electronic debit transaction* . . . ." EFTA § 920(a)(1). The amount of the fee "shall be reasonable and proportional to the cost incurred by the issuer with respect to *the transaction*." EFTA § 920(a)(2). The statute further clarifies that the Board "shall" "distinguish" between incremental

[60] Indeed, TCF agrees that the statute is unambiguous, arguing as follows in its preliminary injunction motion: "The statute explicitly forbids regulated banks from charging retailers for 'any cost' of a debit transaction other than those three electronic steps: in other words, it excludes variable costs that are needed to service the customer's account, and all fixed costs that are incurred in order to establish, maintain and operate the system." TCF Mem. in Support of Prelim. Injunction, Docket No. 16 at 2, *TCF Nat'l Bank v. Bernanke*, No. 10 Civ. 4149 (D.S.D. Nov. 4, 2010).

[61] While the intent of Congress is clear on the face of the Act, Senator Durbin's comments on the Senate floor also confirm this intent: "Paragraph (a)(4) makes clear that the cost to be considered by the Board in conducting its reasonable and proportional analysis is the incremental cost incurred by the issuer for its role in the authorization, clearance, or settlement of a particular electronic debit transaction, as opposed to other costs incurred by an issuer which are not specific to the authorization, clearance, or settlement of a particular electronic debit transaction." 156 Cong. Rec. 105, S5925 (July 15, 2010).

ACS costs "of *a particular* electronic debit transaction, which cost shall be considered," and "other costs incurred by an issuer which are not specific to *a particular* electronic debit transaction, which costs shall not be considered . . . ." EFTA 920(a)(4)(i & ii) (emphasis added).

The suggestion that there are permissible "transaction costs" other than incremental ACS costs that the Act does not address cannot withstand scrutiny. This is apparent from Visa's complete failure to identify one credible example of such costs. Visa's examples – "the costs of printing cards and mailing statements" – plainly cannot be considered incremental or transaction-specific costs under any common sense meaning of those terms.[62] In fact, Visa telegraphs the weakness of its position when it invites the Board to ignore the Act completely and consider all issuer costs because "any cost incurred by an issuer with respect to its debit card program facilitates its debit card transactions in some manner."[63] As the plain text and structure of the Act is not ambiguous, the Act does not permit the conclusions set forth in Visa's submission.

After suggesting that the Board ignore the Act and consider all issuer costs, Visa then proposes that the Board set an industry wide "Average Effective Debit Interchange" rate, and permit networks to set debit interchange rates above or below the "Average Effective Debit Interchange Rate" as long as the network's system-wide rates are not higher than the "Average" rate.[64] This is a thinly veiled invitation to perpetuate the current system, and in particular Visa's (and other

---

[62] Visa Letter at 14.

[63] *Id.*

[64] Visa Letter at 18.

network's) ability to price discriminate against CNP merchants. As Visa acknowledges, "under this approach, a network could set different rates based on merchant size, merchant segment, acceptance channel (e.g. card present vs. card not present)."[65] Once again, Visa reaches this conclusion only by ignoring the Act as well as Congress's clear intent in passing it. Congress made clear that it passed the Act to cabin Visa's and MasterCard's market power over merchants.[66] Any result that enables continuing price discrimination against CNP (or other merchants) – indeed, price discrimination is classic indicia of market power[67] – flies in the face of the Act and its clear objectives. Visa's attempt to perpetuate the current discrimination against CNP merchants should be rejected.

II. A Fraud Adjustment Should Be "Reasonably Necessary" Only When Issuers Implement Systems That Give Them the Confidence to Accept Full Chargeback Responsibility

Allowing issuers to recover positive interchange in the form of fraud adjustments related to current technology will perpetuate the current system which penalizes Internet merchants – especially merchants such as Dell that likely do more than debit issuers to secure payment card transactions on their sites. It will also extend a problematic system where the issuers that are best positioned to police fraud have inadequate incentives to do so. Accordingly, the Board should

---

[65] *Id.*

[66] *See* note 40, quoting Senator Durbin's comments on the Senate floor concerning interchange as a demonstration of market power.

[67] *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".).

not allow any fraud adjustments unless issuers implement technology with which they have sufficient confidence to accept full responsibility for the transaction by taking all chargeback risk. And even in that circumstance, merchant fraud prevention, chargeback, and PCI costs should be counted as an offset or deduction from any claimed positive interchange. At a minimum, issuers should not be allowed to recover any positive interchange in the guise of a fraud adjustment until fraud prevention and PCI costs from merchants such as Dell are taken into account.

The Act places stringent conditions on any adjustments to interchange based upon fraud prevention costs under EFTA § 920(a)(5). First, adjustments must be "reasonably necessary" to compensate for fraud costs related to an issuer's debit transactions. EFTA § 920(a)(5)(A)(i). Second, issuers must meet adjustment standards adopted by the Board which ensure that such costs are in fact limited to fraud prevention. EFTA § 920(a)(5)(A)(ii)(I). Third, adjustment standards must take into account fraud-related reimbursements from all parties – expressly including chargebacks paid for by merchants. EFTA § 920(a)(5)(A)(ii)(I). Fourth, the adjustment must take into account "fraud prevention and data security costs" expended by merchants and others. § 920(a)(5)(B)(ii)(IV). Lastly, adjustment standards must require that issuers "take effective steps" to reduce fraud and fraud prevention costs, including through the development of "cost-effective fraud prevention technology." EFTA § 920(a)(5)(A)(ii)(II).

The Act also expressly sets out several factors which the Board must consider in adopting standards for any fraud adjustment. EFTA § 920(a)(5)(B)(ii). These considerations require any adjustment standards to confront the deep flaws of the current system under which issuers and payment networks have discouraged the use and development of effective and secure technology for Internet transactions.[68] After consideration of the factors enumerated under the Act, at a minimum, it is clear that any positive fraud adjustments for investments related to current technology used over the Internet would only perpetuate the problematic incentives of the current system.

Consistent with the requirement that adjustments be limited to "reasonably necessary" and "effective" technological steps, EFTA § 920(a)(5)(A)(ii)(II), effective fraud technology under this standard should be limited to technology that is sufficiently secure such that issuers would be willing to absorb all chargeback risks. This approach will assure that positive interchange will only be provided if issuers take appropriate steps by implementing new technology that will enable them to accept full responsibility for all transactions. The fraud that is caught by merchants should be compared to the effectiveness of the issuer's system. As such, the millions in potential fraud that Dell diverts from the system ([DELL CONFIDENTIAL & PROPRIETARY INFORMATION]) after issuers have authorized the transactions – along with that of other CNP merchants – should be considered before positive interchange is awarded to issuers. Only if the issuers' system is more effective than the systems of CNP merchants should

[68] The Act directs the Board to consider past incentives or lack of incentives to reduce fraud under the existing interchange system. EFTA § 920(a)(5)(B)(ii)(VI).

interchange be awarded. Moreover, the approach should be issuer-specific to generate issuer competition. *See* EFTA § 920(a)(5)(A)(i) ("such adjustment is reasonably necessary to make allowance for costs incurred *by the issuer* in preventing fraud in relation to electronic debit transactions *involving that issuer*") (emphasis added). As such, fraud prevention systems should not be imposed on merchants via network rules that are tied to acceptance or network-imposed liability shifts.

Lastly, before issuers receive positive interchange under any such fraud adjustment, merchant chargeback, fraud prevention and PCI costs must be taken into account as an offset or a deduction.[69]

[69] In the alternative, if the Board concludes that some form of risk-based pricing is justified for certain merchants under the fraud adjustment, that approach should be limited to merchants, Internet or brick-and-mortar, who create high risks because of the way they operate. While Dell thinks such risk based pricing is not warranted under any circumstances, to the extent the Board is inclined to permit this approach going forward with debit transactions, it should be applied based on merchant risk and not based on whether the merchant operates over the Internet.

CONCLUSION

To summarize our conclusions:

- The interchange pricing distinction between card-present and CNP merchants should be eliminated. Whether debit interchange be set at par or limited to the issuer's nominal ACS costs, the result should apply equally to all merchants.

- The Board should set standards that render an adjustment for fraud prevention "reasonably necessary" only when the issuer has taken "effective steps" to reduce fraud such that the issuer would be prepared to absorb all or virtually all chargeback risks for cardholder fraud after the "effective steps" have been implemented. Merchant fraud prevention and PCI costs should be deducted from any such adjustment.

Dell respectfully requests an in-person meeting at the Board's convenience in advance of the Notice of Proposed Rulemaking to discuss these issues. In advance, we appreciate your attention to our submission.

Differential Between Card Present and Card Not Present Visa Debit Interchange Fees[1]

	Oct-01	Apr-02	Oct-02	Apr-03	Nov-06	Oct-07	Oct-09	Apr-10	Oct-10
Card Present Interchange Rates									
CPS Retail	1.38%+$.05	$1.38+$.05	1.37%+10	1.39%+$.10	1.03%+$.15[2]	1.03%+$.15	1.03%+$.15	0.95%+$.20	0.95%+$.20
CPS Retail - Volume Threshold 1[3]						0.62%+$.13	0.62%+$.13	0.62%+$.13	0.62%+$.13
CPS Retail - Volume Threshold 2						0.81%+.13	0.81%+.13	0.81%+.13	0.81%+.13
CPS Retail - Volume Threshold 3						0.92%+$.15	0.92%+$.15	0.92%+$.15	0.92%+$.15
Card Not Present ("CNP") Interchange Rates									
CPS Card Not Present	1.80%+$.10	1.80%+$.10	1.80%+$.10	1.80%+$.10	1.60%+$.15	1.60%+$.15	1.60%+$.15	1.60%+$.15	1.60%+$.15
CPS eCommerce-Basic	1.80%+$.10	1.80%+$.10	1.80%+$.10	1.80%+$.10	1.60%+$.15	1.60%+$.15	1.60%+$.15	1.60%+$.15	1.60%+$.15
CPS eCommerce-Preferred	1.80%+$.10	1.80%+$.10	1.80%+$.10	1.80%+$.10	1.55%+$.15	1.55%+$.15	1.55%+$.15	1.55%+$.15	1.55%+$.15
Differential Between Card Present and Card Not Present Interchange Rates									
CNP Basic minus Retail	**.42%+$.05**	**.42%+$.05**	**0.43%**	**0.41%**	**0.57%**	**0.57%**	**0.57%**	**0.65%-$.05**	**0.65%-$.05**
CNP Basic minus Retail Threshold 1						**0.98%+$.02**	**0.98%+$.02**	**0.98%+$.02**	**0.98%+$.02**

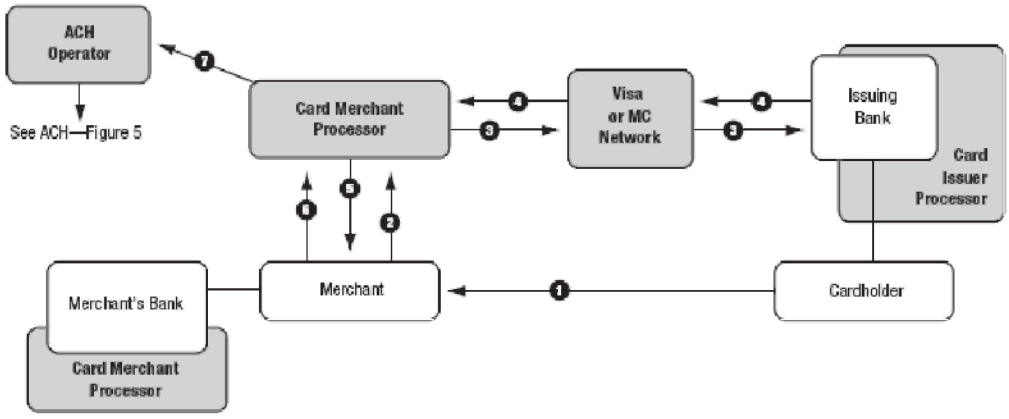
[1] Source: Electronic Transaction Association, Visa. As the chart reflects, CNP interchange rates have not meaningfully declined over the years despite numerous improvements in fraud prevention for Internet transactions.

[2] Debit interchange fees declined by 2004 as part of the Visa Check/MasterMoney Antitrust Litigation settlement. For a chart of card-present debit interchange from 1996-2006, noting this decline, see Fumiko Hayashi, Richard J. Sullivan, and Stuart E. Weiner, *A Guide to the ATM and Debit Card Industry* at 13, Fig. 8, http://www.kansascityfed.org/PUBLICAT/PSR/BksJournArticles/ATMDebitUpdate.pdf.

[3] CPS Retail rates now include a number of sub-classifications based upon transaction, sales volume, and chargeback ratio. For example, Threshold 1 requires 52 million transactions, $3.4 billion in sales, and chargeback rate lower than .015%. *See http://usa.visa.com/download/merchants/october-2010-visa-usa-interchange-rate-sheet.pdf.*

APPENDIX 2[4]

Figure 6: Credit & Offline Debit: Card Present—Visa/MasterCard Networks



Authorization

1. A consumer uses a credit card to pay a merchant.
2. The merchant sends the encrypted transaction data to a card merchant processor (e.g., First Data Merchant Services) for authorization.
3. The card merchant processor sends the transaction data to the consumer's (issuing) bank over the Visa or MasterCard network. The issuing bank is a licensed member of Visa or MasterCard and holds agreements with, and issues cards to, consumers.
4. The issuing bank authorizes the amount and issues an authorization code or declines the transaction.
5. The card merchant processor notifies the merchant that the transaction either has been authorized or declined. The merchant requests the consumer's signature as authorization for the transaction or notifies the consumer that the transaction has been declined.

Processing

6. Once authorized, the transaction must be "captured" by the merchant. The capture uses information from the successful authorization to charge the authorized amount of money to the consumer's credit card. The merchant accumulates captures and credits into a batch, which then will be settled as a group. The merchant submits the batch to the card merchant processor to finalize the transactions. (If the consumer returns goods after a transaction has been captured, a "credit" is generated.)

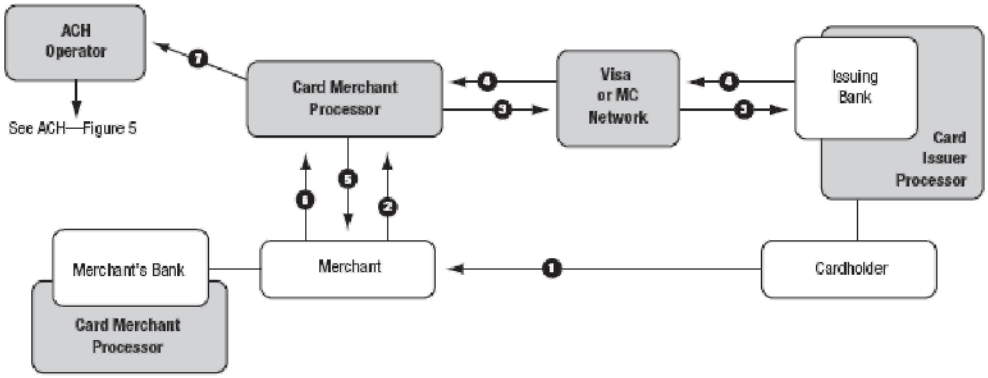
Settlement

7. The card merchant processor receives the information and settles the batch, then sends ACH items through the ACH operator to the issuing and merchant banks. (See Figure 5; the merchant bank is the ODFI, with the card merchant processor serving as authorized sending point.) The operator settles transactions between the issuing and merchant banks. The merchant bank credits the merchant's account.

Note: Many merchant banks hire a third party (acquiring processor) for bankcard processing. The processor provides credit card processing, billing, reporting and settlement, and operations services to the merchant bank.

[4] Terri Bradford et al., *Nonbanks in the Payments System*, 24, 26 (Nov. 2003).

Figure 1: Credit & Offline Debit: Card Not Present



Authorization

1. A consumer uses a credit card to make a purchase from a merchant's Web site. The merchant's e-commerce-enabled Web site prompts the consumer for credit card information and "bill to" and "shipping" addresses.
2. The merchant sends the encrypted transaction data to a merchant acquiring processor (e.g., First Data Merchant Services) for authorization.
3. The acquiring processor sends the transaction data to the consumer's issuing bank over the Visa or MasterCard network. The issuing bank is a licensed member of Visa or MasterCard that holds agreements with and issues cards to consumers.
4. The issuing bank authorizes a certain amount of money and issues an authorization code or declines the transaction.
5. The acquiring processor communicates with the merchant's Web site, which notifies the customer that the transaction is either authorized or declined.

Processing

6. Once the transaction has been authorized, it must be captured. The capture uses information from the successful authorization to charge the authorized amount of money to the consumer's credit card. The merchant accumulates captures and credits into a batch and settles them as a group. When submitting a batch, the merchant's payment-enabled Web server connects with the acquiring processor (e.g., First Data) to finalize the transactions.

Settlement

7. When the acquiring processor receives the information and settles the batch, it sends ACH items through the ACH operator to the issuing and merchant banks. (See Figure 5: the merchant bank is the ODFI, with the acquiring processor serving as authorized sending point.) The operator settles these transactions between the issuing and merchant banks. The merchant bank credits the merchant's account. (If the consumer returns goods after a transaction has been captured, a "credit" is generated.)

Note: Many banks hire a third party (acquiring processor) for bankcard processing. The processor provides credit card processing, billing, reporting and settlement, and operational services to the acquiring bank.