November 20, 2010

By Electronic Delivery

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

Re: Rulemaking Pursuant to EFTA Section 920

Dear Ms. Roseman:

On behalf of Amazon.com, Inc. ("Amazon"), I respectfully write to provide information to assist the Board of Governors of the Federal Reserve System (the "Board") in its rulemaking pursuant to Section 920 of the Electronic Fund Transfer Act ("EFTA" or the "Act"). This section of the Act requires the Board to set standards to ensure that any interchange received or charged by regulated debit issuers is "reasonable and proportional" to costs. As described and supported in this letter, the current interchange pricing discrimination between so-called "card-present" and "card-not-present" debit card transactions must be eliminated under the Act.[1]

More specifically, Amazon believes that interchange is only "reasonable" if issuers would not issue debit cards at all without it. Because issuers would continue to issue debit cards even without interchange, interchange should be set at par. This result should apply to all debit transactions irrespective of the merchant or merchant category in which the transaction takes place. The elimination of discriminatory treatment would also apply if the Board permits issuers to recover their incremental costs of authorizing, clearing and settling debit transactions. Those costs do not vary much, if at all, based on the merchant category in which the transaction is consummated, and the argument that the costs are greater for card-not-present transactions does not withstand serious scrutiny. As a result, rules faithful to the Act must eliminate the card-present/card-not-present distinction for debit transactions because it cannot be justified as

[1] Although Amazon objects to the term "card-not-present" because it has been used as a rationale to justify the imposition of discriminatory interchange and chargeback rules on Internet, mail, telephone, and television order-based merchants, I use the term in this letter for convenience. Moreover, although Amazon believes the present/not-present distinction should be eliminated for all payment card transactions, we recognize that the Act's mandatory scope is limited to certain electronic debit transactions. EFTA § 920(a), (c)(2),(5). We hope that eliminating this unfair distinction for debit transactions eventually will lead to ending the practice entirely.

reasonable or proportional to the cost incurred by issuers with respect to card-not-present transactions. Our specific conclusions are as follows:

- The interchange pricing distinction between card-present and card-not-present debit transactions must be eliminated because it is neither "reasonable" nor "proportional" to the issuers' costs that the Board may consider under the Act. We agree with other commentators that electronic debit transactions be interchanged at par.
- If the Board determines that issuers should receive some interchange fee for electronic debit transactions, the amount of that interchange must be limited to the actual and nominal costs of authorizing, clearing and settling debit transactions. Because the costs of performing these services do not vary materially across merchants, the resulting rates must be applied equally to all transactions, regardless of the location of the merchant's storefront, in order to be "reasonable" and "proportional" as required by the statute.
- The Board should set standards that allow an adjustment for fraud prevention as "reasonably necessary" only when the issuer has taken "effective steps" to reduce fraud, and the issuer absorbs all or virtually all chargeback risks for fraud. Moreover, the standards should be performance-based and technologically neutral since there are numerous ways fraud can be reduced with respect to card-not-present transactions and the market should make those decisions.
- Lastly, consistent with the statute, no issuer may receive a fraud adjustment under the Act until a merchant's fraud prevention, Payment Card Industry Data Security Standard (PCI DSS) and chargeback costs have been deducted from any fraud adjustment claimed by an issuer. In other words, if issuers bore the entire cost of preventing fraud, it would be appropriate to adjust for fraud prevention. If, however, a merchant bears both the risk of fraud and the cost of fraud prevention (as is currently the case), allowing issuers a fraud adjustment is neither fair nor rational.

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

Since the Internet became a commonly used medium for commerce in the 1990s, the payment industry has required Internet merchants (often grouped with telephone/mail merchants and referred to as card-not-present merchants) to pay higher interchange rates than the rates paid by their direct competitors operating solely in traditional brick-and-mortar environments. (See Appendix 1 for a comparison of card-present and card-not-present interchange rates since 2001.) This practice was justified by the purportedly higher risks card-not-present transactions created for the system, a justification that, if it was ever valid, has vanished over time.

The inequities inherent in the 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 and policies imposed by the payment card brands.[2] The

[2] Card-not-present or Internet merchants typically contest only 50 percent of chargebacks, and they succeed only 40 percent of the time. 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. Thus, overall, card-not-present merchants

chargeback rules give merchants the ability to represent (i.e., dispute) a chargeback if they can produce a signature and verify that they complied with the rules at the point of sale. The rules were generally not designed to accommodate the different data that Internet merchants use to authenticate the identity of the customer. Internet merchants thus have little ability to contest chargebacks, in contrast to brick-and-mortar merchants, even in situations where the authentication factors are as strong if not stronger than a signature at the point of sale. As a result, in addition to paying higher interchange fees than bricks-and-mortar merchants, card-not-present merchants absorb the vast majority of the fraud costs associated with payment card transactions.[3] This reality was acknowledged by Richard Sullivan of the Reserve Bank of Kansas City in his 2010 study that 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 card-not-present transactions."[4]

Compounding this inequity, the higher interchange paid by card-not-present merchants has continued to penalize those merchants that have developed their own authentication technologies that effectively manage risk. This unjustified and discriminatory structure has remained 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.[5] In fact, established merchants like Amazon have made a substantial investment in fraud management systems, which has resulted in fraud rates that are equal to or better than many brick-and-mortar merchants.

Section 920 of the Electronic Funds Transfer Act

In order to constrain the networks' (and issuers') market power over merchants,[6] Congress recently amended the EFTA to require the Board to promulgate rules that issuers will

---

absorb 80 percent of chargebacks. Jane Adler, *Checking the Chargeback Scourge*, Digital Transactions at 36 (chart), 38 (June 2010), http://www.digitaltransactions.net/files/DigitalTransactionsJune2010.pdf.

[3] An increasing portion of the chargebacks Internet merchants face is the result of so-called "friendly fraud," where cardholders can exploit the networks' zero liability policy to repudiate a transaction that he/she made or that a relative made and force the merchant to absorb the loss, because the merchant likely cannot represent the chargeback in most instances. This category of fraud represents a substantial and increasing portion of the chargebacks received by card-not-present merchants, particularly for digital goods or subscriptions where cardholders may have learned to game the system improperly based on their bank's liberal policies. 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).

[4] 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.

[5] We note that, notwithstanding certain catalog, television, and other non-Internet card-not-present merchants' low chargeback rates and sophisticated fraud management systems, this two-tier system has applied to them for an even longer period of time.

[6] *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

be required to follow in setting interchange for debit transactions. *See* EFTA § 920. The framework Congress laid out in EFTA Section 920 is as follows:

(1) The amount of interchange an issuer may receive or charge with respect to an electronic debit transaction must be "reasonable and proportional to the cost incurred by the issuer with respect to the transaction." EFTA §920(a)(2);

(2) In setting rules for interchange, the Board must consider the similarity between electronic debit transactions and checking transactions, which are required to clear at par. EFTA §920(a)(4)(A);

(3) In determining whether interchange is "reasonable and proportional" to costs, the Board *may* consider "the incremental costs incurred by an issuer" for the issuer's role in "authorization, clearance or settlement" of a particular electronic debit transaction, EFTA §920(a)(4)(B)(i), but *may not* consider "other costs incurred by an issuer which are not specific to a particular electronic debit transaction." EFTA §920(a)(4)(B)(ii); and

(4) The Board *may* allow for an adjustment to interchange for "fraud prevention costs" *if:*

   a. the adjustment is "reasonably necessary" to cover costs incurred by the issuer "in preventing fraud in relation to electronic debit transactions involving that issuer." EFTA §920(a)(5)(a)(i); *and*

   b. the issuer complies with fraud-related standards set forth by the Board that are:

      i. designed to ensure that any adjustment is limited to what is "reasonably necessary" and takes into consideration any "fraud-related reimbursement," including amounts received via chargebacks; *and*

      ii. require issuers to take effective steps to reduce the occurrence of and cost of fraud in relation to debit transactions, including through the development of cost-effective fraud prevention technology. EFTA §920(a)(5)(A)(ii).

(5) In determining what, if any, fraud adjustment is allowable, the Board must consider:

   a. the nature, type and occurrence of fraud in electronic debit transactions and the extent to which the occurrence depends on how authorization occurs;

   b. the fraud prevention and data security costs expended by each party to the transaction as well as which party absorbs the cost of fraudulent transactions; and

   c. past incentives or lack of incentives to reduce fraud under the existing interchange system. EFTA §920(a)(5)(B)(ii).

---

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.

In short, Congress has directed that the interchange fee that may be charged for an electronic debit transaction be reasonable and proportional to the actual cost of completing the transaction and that the cost of fraud may only be considered to the extent the issuer has taken steps to effectively address fraud and has not already been reimbursed for the cost of that fraud.

The payment industry has historically relied on the distinction between "card-present" transactions and "card-not-present" transactions as a proxy for the "cost" of a transaction, thereby justifying charging much higher interchange fees for "card-not-present" transactions regardless of the actual cost to the network of any individual "card-not-present" transaction. Congress has made clear in these amendments to EFTA that this false proxy be eliminated. An analysis of how this false proxy impacts a high-quality, low-fraud merchant like Amazon.com highlights that the Board should require the elimination of this artificial distinction.

About Amazon.com

Amazon.com opened its virtual doors on the World Wide Web in July 1995 and offers "Earth's Biggest Selection" of goods online. Amazon seeks to be Earth's most customer-centric company for three primary customer sets: consumers, sellers, and developers. It serves consumers through its retail websites, and focuses on selection, price, and convenience.

Amazon designs its websites to enable millions of unique products to be sold by Amazon and by third parties across dozens of product categories. It strives to offer customers the lowest prices possible through low everyday product pricing and free shipping offers, and to improve operating efficiencies so that it can continue to lower prices for its customers.

Amazon's retail customers in the United States purchase items through its retail websites, where payment options include credit card, debit card, bank accounts, Amazon.com gift cards and gift card codes, and the Amazon store card. While the use of alternative payment methods such as gift cards and bank accounts is growing, over 90% of U.S. transactions are paid for using credit or debit cards.

Providing a safe and secure experience for customers is of paramount importance to Amazon. As a result, in the last three years alone, Amazon has invested [AMAZON CONFIDENTIAL & PROPRIETARY INFORMATION] in direct fraud prevention measures designed to prevent fraud on its websites worldwide.[7]

As a result, Amazon experiences fraud rates that are equal to or better than the average experience of brick-and-mortar merchants. [AMAZON CONFIDENTIAL & PROPRIETARY INFORMATION] This rate is at least equivalent to industry standard rates for brick-and-mortar merchants.[8] Based on the published rates (set forth in Appendix 1), Amazon pays on average 98

[7] Note that this amount does not include the cost of service dedicated to fraud prevention by groups whose direct charter is not limited to fraud prevention, such as customer service, information security, global payments services, infrastructure, etc.

[8] Amazon is not aware of any current, publically available data regarding the average fraud chargeback rate experienced by brick-and-mortar merchants. However, based on historic data and reports, the rate is likely between 5 and 10 basis points. *See, e.g.*, Merchant Risk Council, Press Release, *Online Fraud Rates Approaching Fraud*

basis points more for interchange fees on electronic debit transactions than a similar brick-and-mortar merchant. This enormous differential in interchange fees cannot be justified by Amazon's fraud rates, which are in line with brick-and-mortar merchants. As a result, the artificially inflated interchange paid by merchants like Amazon for card-not-present transactions cannot be reasonable or proportional to the cost of those transactions or "reasonably necessary" to cover the cost of any fraud prevention that issuers actually provide.

While Congress has made clear that miscellaneous costs (unrelated to authorization, clearance and settlement) cannot be considered when setting interchange, it is important to note that high-quality merchants like Amazon bring fewer of those costs to the network as well. The customer experience is of paramount importance to Amazon, so it has:

- clear product and condition disclosures;
- clear pricing policies and disclosures;
- clear returns policies and disclosures;
- efficient order processing;
- strong delivery and shipping promises, which it adheres to; and
- top-tier customer service.

Consequently, Amazon does not burden the network with increased customer service costs.

In short, Amazon is a high-quality merchant that invests tens of millions of dollars in fraud prevention (not to mention customer service), and has a fraud prevention rate that rivals any merchant in the industry. Yet networks and issuers charge Amazon interchange fees for debit transactions (and credit transactions) that are on average 98 basis points higher than a similar brick-and-mortar merchant simply because issuers use the proxy of "card-not-present" to categorize Amazon's transactions. The Board must implement rules under the framework established by Congress in the recent amendment to Section 920 that do not allow this inequity to persist.

Reasonable and Proportional Interchange Should Be Set at Par

Under the Act, interchange must be both "reasonable" and "proportional" to the cost incurred by the issuer with respect to the transaction. EFTA § 920(a)(2). To be "reasonable" interchange must be found necessary to motivate issuer participation in the system. Indeed, the Act directs the Board to consider the functional similarity between checks and debit cards as access devices to demand deposit accounts. EFTA § 920(a)(4)(A). That is because banks have

---

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."). More precise data should be provided by the issuers and payment card brands to assist the Board in evaluating the reasonable costs necessary to cover fraud prevention. Richard Sullivan, among others, has noted the need for better data collection in this area. *See* Sullivan, *Changing Nature of U.S. Card Payment Fraud* at 121-22; *see also* Richard J. Sullivan, *The Benefits of Collecting and Reporting Payment Fraud Statistics for the United States* (October 2009), http://www.kansascityfed.org/PUBLICAT/PSR/Briefings/PSR-BriefingOct09.pdf.

long issued checks without interchange. Banks do this presumably for convenience and customer relationship purposes because they give consumers remote access to their money without credit risk. The rationale for providing customers access to bank accounts via electronic debit transactions is no different, so the only "reasonable" debit interchange is at par. Not surprisingly, debit issuance thrives around the world, including in Canada, without interchange.[9] It is clear that debit interchange in the United States is nothing more than a subsidy from the merchant to the issuer that cannot be justified. Accordingly, debit interchange should be at par, and the separate rates that apply to card-not-present merchants must be eliminated by the standards set under the Act.

If Interchange is Allowed, It Must Be Limited to the Nominal Costs of Authorization, Clearance, and Settlement, Which Is Virtually the Same for All Merchants

If the Board concludes that some form of interchange above par is "reasonable," it must then establish standards to ensure that the rates set are "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" that are "not specific to a particular electronic debit transaction . . . ." EFTA § 920(a)(4)(B)(i & ii). The incremental costs that may be considered are those incurred with respect to the specific debit transaction. No fixed, average, lifetime, indirect, or amortized costs can be considered.[10]

These "authorization, clearance, or settlement" costs ("ACS" costs) must be limited to the incremental processing costs associated with authorizing the transaction (*i.e.*, confirming whether the cardholder has sufficient funds to complete the purchase), clearing the transaction (*i.e.*, delivering final transaction data that issuers can post to the cardholder's account), and settling the transaction (*i.e.*, calculating the final net financial position of issuers and acquirers). Consideration of any costs that do not meet these statutory requirements, including the cost of fraud, is explicitly disallowed by the statute. Congress anticipated that issuers would try to include fraud prevention costs in ACS costs, but was clear in its intention to exclude consideration of these costs from the determination of "reasonable and proportional" interchange.[11] As Senator Durbin stated when discussing the Act on the Senate floor, "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

[9] In Canada, notably, the Interac debit network is now facilitating Internet transactions without interchange.

[10] In its recent preliminary injunction motion to stop enforcement of the Act, TCF Bank agrees that the statute is unambiguous, arguing "[t]he 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).

[11] Contrary to the Act, issuers are undoubtedly trying to expand the meaning of the term "authorization" beyond recognition to include fraud prevention costs. *See, e.g.*, Wells Fargo, *Debit Card Discussion with Federal Reserve Board* at 6 (Sept. 1, 2010) (setting forth "POS Authorization Flow" which appears to include "fraud and risk systems").

prevention costs would not be considered as part of the incremental issuer costs upon which the reasonable and proportional amount is based."[12]

Excluding fraud prevention costs from the calculation of authorization costs is consistent with the generally accepted meaning of the term "authorization" in the industry. "Authorization" means confirming that the funds are available to complete the purchase. This is apparent from Visa's description of authorization in the website for Visa's Debit Processing Service ("DPS"), which offers authorization and fraud prevention services for issuers. Visa defines "stand-alone authorization" to include decisions based on "activity limits and account balances"– the basic criteria to confirm the availability of funding.[13] Various fraud prevention tools, tellingly, are sold as additional tools that issuers may select.[14] Visa DPS, for example, includes a number of customizable fraud systems that – at the issuer's option – may be accessed as add-ons during authorization processing.[15] This reinforces the conclusion that the industry recognizes that the core function of "authorization" is checking for the availability of funds – and not fraud prevention.[16]

If there were any doubts about what the term "authorization" means, the Board need only consult the neighboring statutory terms, "clearance" and "settlement." These are also narrow concepts that, based upon their established meaning, are limited to the processing associated with delivering transaction data and calculating net financial positions. 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)). Thus, the meaning of the term "authorization" should not be considered in isolation apart from the full phrase, "authorization, clearance, or settlement." Fraud prevention does not appear anywhere in the commonly understood meanings of any of these terms.

As commonly understood in the industry, authorization, clearance, and settlement are substantially the same for all debit transactions whether card-present or card-not-present. *See* Terri Bradford et al., *Nonbanks in the Payments System*, 24-26 (Nov. 2003) (A publication of the Federal Reserve Bank of Kansas City, which includes several flowcharts that explain the steps of "authorization," "processing" and "settlement."). [17] These costs are flat transaction costs that do not vary by merchant type, so the distinction between card-present and card-not-present transactions cannot be justified and must be eliminated.

---

[12] 156 Cong. Rec. 105, S5925 (July 15, 2010).

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

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

[15] *Id.*

[16] We think it is important not to conflate "credit risk" prevention, which is a component of authorization, and "fraud risk" prevention, which is a component of authentication. Conflating credit risk and fraud risk could lead to the inclusion of authentication costs in authorization, clearance and settlement costs, which is not permitted by the statute.

[17] See Appendix 2 to November 18, 2010 Submission of Dell, Inc.

The Network and Issuer Arguments to Perpetuate Higher Card-Not-Present Interchange for Debit Are Groundless

Based upon their submissions to the Board, networks and issuers appear to be exaggerating any potential difference, no matter how slight, between card-present and card-not-present transactions to justify a higher interchange fee for card-not-present 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 merchants. *Presentation to the Federal Reserve on Debit Card Regulation* at 12 (July 23, 2010). A careful parsing of Visa's arguments makes it clear that the notion that slight variations in processing environment for the millions of Internet transactions somehow justifies higher interchange for card-not-present transactions cannot withstand scrutiny.

Visa tries to justify higher interchange for card-not-present transactions by pointing to the following supposed issues associated with card-not-present transactions: 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 card-not-present transactions cannot be fulfilled in one shipment and, thus, may generate partial reversals and separate authorizations, potentially increasing the cost of the total transaction. As an initial matter, the relatively nominal costs of the transaction cannot possibly justify the differential between card-not-present and card-present merchants. While Visa highlighted only the potential extra costs of partial reversals and additional authorizations for card-not-present transactions (attributed to split shipments), it completely ignores the host of other card-present transactions that also have potential for increased reversals and authorizations due to their unique business needs. Given that no other merchants pay interchange as high as card-not-present merchants, this reinforces the conclusion that this justification for higher card-not-present interchange is specious.

Merchant Data Collection. According to Visa, card-not-present transactions 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 Order Number" and "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 card-not-present merchants – is trivial, however, and is part of existing transaction messaging for card-present transactions as well.[18] As such, this issue does not support maintaining the distinction between card-not-present and card-present transactions.

Verification Services. Visa fares no better with its suggestion that services such as checking address verification (AVS) or card verification number (CVV2) somehow justify additional interchange. These are fraud prevention costs that under the Act cannot be counted in the ACS calculation. In addition, merchants already pay for these services, and cannot be

[18] 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.

required to pay twice for their integration into the ACS process.[19] Finally, brick-and-mortar merchants increasingly use AVS and request customer zip codes at the point of sale, and thus these are not technologies solely used for card-not-present transactions.

Customer Service Calls. Visa lists "[i]ncreased customer service calls" as an impact on issuers processing card-not-present transactions. Under the Act, these costs cannot be counted as ACS costs for two 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 for the Board to police.

Using customer service costs to justify higher interchange for card-not-present merchants makes no sense when one considers that high-quality merchants like Amazon, which offers low-risk, high-quality merchandise with customer friendly sales and support practices, are deemed suspect while low-quality merchants that offer high-risk products but operate in the bricks-and-mortar environment get a free pass. The result of the current structure is that high-quality merchants whose business is limited to card-not-present transactions subsidize low-quality (and even fraudulent) merchants across merchant categories. Visa's argument concerning customer service calls is without merit and must be rejected by the Board.

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

Congress has mandated that a fraud adjustment to interchange can only be considered if it is "reasonably necessary" to make allowance for fraud prevention costs borne by the issuer as a result of debit transactions by that issuer. For a fraud adjustment to be "reasonably necessary," it should compensate issuers for providing a service that merchants value and are either unwilling or unable to provide for themselves. As a result, we propose that before a fraud adjustment can be considered, issuers should be required to accept full liability for cardholder fraud.[20] The principle is simple: if issuers do not trust their fraud prevention technology enough to take complete responsibility for cardholder fraud, it is not reasonably necessary and they should receive no fraud adjustment for that technology. Our proposal is grounded in the statute and will facilitate competition among issuers to provide the most effective – and cost effective – fraud prevention technology. In addition, this approach will correct the misaligned incentives in the current system, which provide issuers with no economic incentive to take meaningful steps to reduce payment card fraud, particularly card-not-present fraud, because they receive interchange fees and deflect chargeback liability regardless of how successful their fraud prevention technology is. As a result, a merchant like Amazon that invests heavily in its own fraud prevention technology subsidizes merchants (and issuers) who do not. Our proposal would eliminate this subsidy and, as required by the statute, specifically recognize the expenditure by merchants to reduce fraud-related costs for issuers.

---

[19] *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).

[20] Under the proposal, issuers would assume liability for all cardholder fraud-related chargebacks. Chargebacks relating to poor merchant service quality or merchant complicity in fraud would not be borne by issuers.

Under our proposal, in order to receive a fraud adjustment, issuers must be confident enough in their own "reasonably necessary" and "effective" fraud prevention technology to accept liability for fraud-related chargebacks. 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 should be defined as any technology that is sufficiently secure that issuers would be willing to accept the risk of cardholder fraud-related chargebacks. Issuers will only develop innovative and effective fraud prevention services if they bear the cost of fraud not prevented; thus, the willingness to provide merchants a complete payment guarantee should be a bedrock principle. If issuers are unwilling to express that degree of confidence in the system, a sophisticated and responsible merchant like Amazon would prefer to continue to own fraud prevention and determine for itself how much money to invest in fraud prevention and what techniques are most effective in keeping fraud costs to a minimum.

Our proposal would stimulate issuer competition. In addition to the prerequisite that issuers take full responsibility for transactions going forward, the standards should ensure increased issuer competition, encourage investment in effective technology, and preserve merchant choice. The standards should make clear that for any service or technology to qualify for an adjustment, it must be deployed by a specific issuer and be offered competitively by that issuer (or its agents or distributors) to merchants. This will ensure that fraud prevention technology will neither be forced upon merchants via network rules nor tied or bundled to network acceptance.[21] If issuers and their service providers compete to develop new cost effective fraud prevention technologies, then the marketplace (*i.e.* merchants) can determine what technology or service is valuable enough to warrant an adjustment to interchange.

Our proposal is technology-neutral, except that any new technology cannot disrupt the Internet user experience. Fraud adjustment standards should not pick winners and losers between competing fraud prevention technologies. Those decisions are best made by the market, *i.e.*, the merchant customers of those services.

By way of example, Visa's Verified by Visa and MasterCard's SecureCode services would not qualify for a fraud adjustment under these principles. As an initial matter, these are network services that Visa and MasterCard have attempted to insinuate into the market through their rules. Products mandated by network rules would not qualify for an adjustment. Moreover, Verified by Visa and SecureCode would likely fail the type of performance based standard advocated by Amazon as the fraud prevention benefits of these services is limited at best.[22] Lastly, because they disrupt the purchasing transaction and because many card-not-present

[21] To the extent networks might compete for issuance by developing fraud prevention systems that issuers can utilize, they can do so under our proposal as long as they do not force merchants to implement them.

[22] Even though these services have been offered for years, they have not been widely adopted. *See* CyberSource 2010 at 8 (showing only 16% of larger Internet merchants use either product). CyberSource – which is now owned by Visa – noted that "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." *Id.* at 9 and chart 3; *see also see Kate Fitzgerald, Report: 3-D Secure Not What Name Suggests*, Am. Banker (Feb. 3, 2010).

merchants like Amazon have developed superior authentication technologies that render these services redundant or unnecessary, the intrusion upon the consumer experience cannot be justified as "reasonably necessary" to reduce fraud. Thus, these products would not be sanctioned by the standards.

Our proposal accounts for fraud costs borne by all parties, as required by the Act. 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). In this regard, the adjustment must also take into account "fraud prevention and data security costs" expended by merchants and others. *Id.* at § 920(a)(5)(B)(ii)(IV). Before issuers receive incremental interchange under any such fraud adjustment, merchant chargeback, fraud prevention and PCI costs[23] must be taken into account as an offset or deduction along with any costs the merchant bears associated with implementing the issuer's technology.

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, that create high risks because of the way they operate. And any fraud adjustment can only be considered after accounting for fraud prevention costs borne by each individual merchant. While Amazon 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 individual risk and not on the irrelevant criterion of whether the transaction occurs over the Internet. And it must specifically recognize the substantial expenditures that merchants such as Amazon make to reduce fraud-related costs for issuers.

Conclusion

To summarize our conclusions:

- The interchange pricing distinction between card-present and card-not-present transactions must be eliminated. Whether debit interchange is set at par or limited to

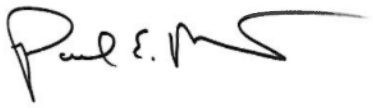
[23] PCI DSS imposes stringent data security requirements on all participants in the payments system. Complying with the standard – which includes some 200 detailed requirements – imposes burdensome costs on merchants, including annual audit and compliance costs and onerous fees and fines that the networks assess in the event of a data breach. However, even when a merchant has gone to the considerable expense of maintaining compliance, if a data breach occurs, the merchant is deemed non-compliant, even if the breach was not the merchant's fault. Given this backdrop, merchants of all stripes consider the PCI system to be one-sided, favoring issuers over merchants. *See* 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 121 (2d Qtr. 2010), http://www.kansascityfed.org/Publicat/Econrev/pdf/10q2Sullivan.pdf; *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.

the issuer's nominal authorization, clearance and settlement costs, in order to be reasonable and proportional, the result must 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 is prepared to absorb all or virtually all chargeback risks for cardholder fraud. Merchant fraud prevention and PCI DSS costs should be deducted from any such adjustment.

Thank you in advance for your attention to the points raised in this letter. I respectfully request an in-person meeting for Amazon payments experts with you or other appropriate Board staff before the Board issues a notice of proposed rulemaking on this matter. Please let me know if you have any questions. I can be reached at pmisener@amazon.com or 202-347-7390. In any case, I will follow up soon to schedule a meeting.

Sincerely yours,



Paul Misener
Vice President for Global Public Policy

APPENDIX 1

Differential Between Card Present and Card Not Present Visa Debit Interchange Fees[24]

	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[25]	1.03%+$.15	1.03%+$.15	0.95%+$.20	0.95%+$.20
CPS Retail - Volume Threshold 1[26]						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**

[24] 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.

[25] 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.

[26] 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.*