

Industry Facts Concerning Debit Card Regulation Under Section 920

**Stephen Craig Mott
BetterBuyDesign**

On Behalf of the Merchants Payments Coalition

**Submitted To
The Board of Governors of the Federal Reserve System
Concerning Its Rulemaking Pursuant To
Section 920 of the Electronic Fund Transfer Act**

October 27, 2010

TABLE OF CONTENTS

I.	INTRODUCTION AND SUMMARY OF CONCLUSIONS	1
II.	DEBIT CARD INDUSTRY BACKGROUND	2
	A. Origins of Debit Cards	2
	B. Early Growth of PIN Debit	3
	C. Signature Debit.....	5
	D. High Positive Interchange Pushes the Market Toward Signature Debit.....	6
	E. The Convergence of Signature and PIN Debit Interchange Rates	12
III.	DISCUSSION OF INDUSTRY FACTS RELEVANT TO RULEMAKINGS.....	16
	A. Banks Will Continue to Issue Debit Cards in a Mature Market Without Interchange.....	16
	<i>i. Banks Make Money on Debit Cards Without Interchange</i>	<i>16</i>
	<i>ii. Debit Cards Displace More Expensive Check and Cash Transactions</i>	<i>18</i>
	B. Debit Card Issuer Costs.....	19
	<i>i. General Costs Versus Authorization, Clearing and Settlement Costs.....</i>	<i>19</i>
	<i>ii. The Remaining Costs of Debit Card Issuance Are Subject to Wide Variations in Reporting and Cost Allocations</i>	<i>20</i>
	C. Industry Data on Fraud.....	24
	<i>i. Merchants Bear a Substantial Portion of the Fraud Costs</i>	<i>24</i>
	<i>ii. Issuers are Best Positioned to Police Fraud.....</i>	<i>33</i>
	<i>iii. Signature Versus PIN Debit Fraud</i>	<i>34</i>
	<i>iv. Fraud in the U.S. Payment System Compared to Other Jurisdictions.....</i>	<i>35</i>
	D. Visa/MasterCard Parallel Conduct in Interchange & Network Fees	35

I. INTRODUCTION AND SUMMARY OF CONCLUSIONS¹

1. I have been asked by counsel for the Merchants Payments Coalition to provide some historical background on the development of the debit market. I also have been asked to supply industry data on certain key issues that might be relevant to the Federal Reserve Board's (the "Board") analysis of the rulemakings and regulations that Congress has asked it to issue under Section 920 of the Electronic Fund Transfer Act. With regard to these issues, I offer the following conclusions:

- The incremental costs of authorizing, clearing and settling debit transactions should be limited to the processing associated with authorizations, *i.e.*, confirming whether the cardholder has sufficient funds to pay for the purchase; the processing associated with clearing, *i.e.*, delivering final transaction data to issuers for posting to the cardholder's account; and the processing associated with settling, *i.e.*, calculating fees and charges that apply to issuers and acquirers, and calculating the net financial position of issuers and acquirers after debit transactions are completed. These processing costs involved with electronically transmitting transaction data are readily identifiable. By contrast, many of the other costs that debit issuers incur are mixed together with other programs, or reflect inefficient outsourcing related to signature debit.
- The incremental costs of authorizing, clearing and settling PIN debit transactions — which occur in a single electronic message — are roughly \$0.0033.² The incremental costs of authorizing, clearing and settling signature debit transactions related to an issuer's DDA system are approximately \$0.0136.³
- Even before PCI DSS costs are taken into account, merchants absorb more of the debit card fraud costs than do issuers. The costs of PCI DSS compliance, alone, for merchants will soon exceed the total cost of payment card fraud in the U.S. To date, merchants have incurred at least \$10 billion in PCI DSS compliance and liability costs.⁴

¹ All documents and deposition testimony referenced herein and preceded by "**Attachment __**" are materials that were either unsealed by the Court in the *In re Visa Check/MasterMoney Antitrust Litigation*, No. 96-CV-5238 (E.D.N.Y.) (J. Gleeson), or are otherwise publicly available. All such materials are appended to this report. Appended as **Attachment 1** is a copy of my curriculum vitae.

² First Annapolis Consulting, "STAR CHEK® Direct Product Overview," Prepared for First Data, June 22, 2004, at 25.

³ First Annapolis POS Debit Issuer Cost Study Comprehensive Report, Presented to First Data and STAR, Oct. 23, 2007, at 26, 28.

⁴ *See infra*, ¶ 53.

- Much of these fraud costs borne by merchants, including PCI DSS and chargeback costs, could be eliminated by the implementation of better fraud prevention technologies.

II. DEBIT CARD INDUSTRY BACKGROUND

A. Origins of Debit Cards

2. Starting in the 1970s, banks began to allow their customers to use personal identification number (“PIN”) debit cards and automated teller machines (“ATMs”) to withdraw funds from their accounts, instead of cashing paper checks. Banks were motivated to offer ATM services in order to reduce their reliance on human tellers and to reduce the number of checks they would have to process. Regional ATM networks soon evolved, which accelerated the ubiquity of ATM services. The banks, using the regional ATM networks, then expanded the utility of the PIN debit system by allowing their consumers to use their debit cards to pay for merchandise at retail stores.

3. Several characteristics made PIN debit appealing to consumers, merchants and banks. Customers benefitted by reducing the amount of cash and checks they needed to carry. PIN debit lessened the need for merchants to process large amounts of cash. Banks eliminated float from checks by processing PIN debit transactions almost immediately, in a single electronic message (which authorized, cleared and settled the transactions instantaneously). Most importantly, banks deployed PIN debit to save money by eliminating the relatively high processing fees associated with paper checks, and they used the additional convenience of PIN debit to strengthen relations with their customers. These deeper relationships motivated customers to maintain higher balances, which banks could profitably loan out. In this way, the value of debit cards to banks vastly transcended the narrow economics associated with the cards. That remains true to this day.

4. Moreover, PIN debit offered banks, merchants and consumers significant security benefits. Because PIN debit required users to enter PINs to initiate the transaction, thieves could not easily use stolen cards to commit fraud. And because PIN debit transactions settled almost immediately, less opportunity existed for consumers to accidentally or intentionally empty their accounts before a given PIN debit transaction settled. This level of security afforded by PIN debit transactions was described by the former CEO of MasterCard as providing a “dramatic lift” over the security offered by signature debit.⁵

5. Because of the high security associated with PIN debit, banks typically have been able to issue PIN debit to the vast majority of their checking account holders.⁶ As detailed more fully below, the incidence of fraud on signature debit transactions has historically been substantially higher than the incidence of fraud on PIN debit transactions.⁷

B. Early Growth of PIN Debit

6. The PIN debit networks worked with banks to promote the growth of debit in the 1970s and 1980s. By the early 1990s, roughly 15 years after PIN and signature debit simultaneously launched, PIN debit accounted for more than 60 percent of all debit transactions.⁸

⁵ **Attachment 2** (Deposition testimony of Alex “Pete” Hart, MasterCard, Aug. 4, 1999) at 249-250.

⁶ **Attachment 3** (Maestro U.S.A., Inc. Board of Directors Agenda Item 13, Mar. 30, 1993, Debit Positioning Strategy) at MD0367-0439 (“Because of its extensive issuance potential to 100% of an institution’s checking account base, on-line [PIN] debit has the ability to maximize retail profitability and access to consumer deposit accounts. MasterCard believes that the issuance capabilities of on-line POS debit coupled with its attractiveness to the merchant community and its low-risk processing environment will make [on-line] POS debit a valuable payment option.”).

⁷ **Attachment 4** (Deposition testimony of George Jeffers, Huntington National Bank, Nov. 8, 1999) at 108 (“there is an infinite amount of more risk involved with an off-line [signature debit] transaction than an on-line transaction”); **Attachment 5** (Deposition testimony of Arthur Kranzley, MasterCard, Feb. 22, 2000) at 61 (testifying that one of the reasons that offline debit had very limited issuance potential in the U.S. in the early 1990s was “because it worked on the MasterCard network, banks had to issue it carefully because of the exposure to risk of fraud ...”); **Attachment 6** (Deposition testimony of Linda Havenor, Visa, July 7, 1999) at 279 (testifying that offline debit presents greater risk to the issuer and greater risk to the cardholder).

⁸ In 1993, PIN and signature debit accounted for 61.3 percent and 38.7 percent, respectively, of total debit purchase transactions in the United States. THE NILSON REPORT (ISSUE 564), Jan. 1994, at 6; THE NILSON REPORT (ISSUE 569), Apr. 1994, at 6-7.

Well into the 1990s, it was common for banks to link to numerous PIN debit networks.

7. To spread the availability of PIN debit, the PIN debit networks encouraged merchants to accept their PIN debit cards. They did this, in part, by subsidizing the costs that merchants incurred in installing PIN pads. In some situations, banks seeking to expand their PIN debit networks paid merchants a small fee for each PIN debit transaction — a practice known as “negative,” “reverse,” or “issuer-paid” interchange. In most situations, however, the PIN debit networks merely set interchange “at par,” offering no subsidy to either merchants or issuers. In fact, at-par pricing was the prevailing norm in the industry throughout the 1980s into the early 1990s.

8. Given its advantages, PIN debit quickly gained a broad level of popularity. Its popularity and reach were aided through the expansion of the regional PIN debit networks. Even Visa recognized that PIN debit was poised to continue to grow, and that it threatened Visa’s core business. In a June 1990 presentation to the Visa board, Visa’s consultant Andersen Consulting predicted the ultimate “demise” of signature debit if PIN debit was “uncontained.”⁹ Andersen also predicted that, if “uncontained,” PIN debit would maintain its at-par interchange structure and thrive with that system.¹⁰

9. MasterCard also recognized the benefits of PIN debit, and planned to incorporate a PIN debit-centered strategy under its rubric. In the early 1990s, MasterCard worked with 12 leading regional PIN debit networks to create Maestro, MasterCard’s PIN debit network. In his October 1991 speech introducing Maestro, former MasterCard chief executive Pete Hart signaled MasterCard’s belief that PIN (online) debit was a superior product to signature (offline) debit,

⁹ **Attachment 7** (Financial Impact of Direct Debit Evolution, Product Development and Marketing Committee, Board of Directors, Visa U.S.A., Andersen Consulting, June 1990) at AND1018612.

¹⁰ *Id.* at AND1018585, AND1018612.

and one to which MasterCard was committed. He stated:

We believe ... in the very simplest of terms at MasterCard ... that debit card should be an on-line business. ... So, we feel that an on-line system with positive identification today, most probably — by virtue of PIN — is the way to provide debit card services to virtually 100% of our deposit or transaction account customers.¹¹

Indeed, MasterCard, at this time, planned to eliminate its offline debit program once Maestro gained acceptance.¹²

C. Signature Debit

10. In 1975, another form of debit card was launched into the market, a product that came to be known as offline debit or signature debit. This form of debit “ran on the rails” of the Visa and MasterCard credit card networks. Rather than using a secure PIN to authorize transactions, this alternate debit system merely required a customer to authenticate his or her identity with a signature. Moreover, rather than authorize, clear and settle transactions in a single electronic message as PIN debit did, this system required two separate messages — the first for authorization and a second to clear and settle transactions. This process created float risks and additional costs for banks.¹³

¹¹ **Attachment 8** (MasterCard International, Pete Hart’s Speech, Oct. 3, 1991) at MD2308-0264–MD2308-0265.

¹² **Attachment 5** (Deposition testimony of Arthur Kranzley, MasterCard, Feb. 22, 2000) at 175-176 (“We saw, even at this time, that Maestro would be our global debit program and that MasterCard [Signature] Debit would probably be phased out as there is more and more acceptance for Maestro.”).

¹³ *Id.* at 58-59 (“The on-line program to us had a number of advantages to the off-line program It also was a PIN-based system so the cardholder was authenticated with each transaction. And the clearing and settlement occurred with the transaction so there wasn’t any float or potential fraud like we had on the off-line system.”). *See also Attachment 9* (Deposition testimony of Linda Gage, Visa, Apr. 27, 1999) at 45 (“The more quickly a transaction is settled, the fewer opportunities we have for disputes, for chargebacks, for fraud. So there is less cost in the system.”); **Attachment 10** (MasterCard Global Deposit Access and Maestro, New Ways to Pay, Oct. 30, 1996) at MD0972-0449 (“Online, real-time posting/clearing of funds virtually eliminates chargebacks; reduces costs & risks”); **Attachment 11** (Visa VCCII - Benefits to Merchants) at 1480653 (“Online, PIN-based transactions are more secure than dual-message (offline), signature-based transactions. Merchants benefit from online processing through lower fraud and chargeback rates. Visa’s support for online processing will expand usage and lower system risk.”); **Attachment 12** (Deposition testimony of Ronald Schmidt, Visa, Mar. 14, 2000) at 360 (“The off-line [debit product] is a higher cost product to the issuer” than the online product.).

11. Between its introduction in the 1970s and 1990, signature debit had limited success. Because a signature-based system introduced risks that were not associated with PIN debit, and because of the float of up to 14 days associated with the clearing and settlement process, banks only issued signature debit to their most creditworthy customers. Given these limitations, by 1990, signature debit cards were viewed as a niche product with, at best, a limited future. By contrast, the prevailing view in the industry was that PIN debit would remain the leading debit product in the United States. For example, according to one of Visa's consultants, if "uncontained," PIN debit would reach "6 billion transactions annually."¹⁴ PIN debit was growing at an annual rate of over 40 percent, and Visa recognized it was poised to take off with or without Visa's participation.¹⁵

D. High Positive Interchange Pushes the Market Toward Signature Debit

12. Visa saw that PIN debit, with its at-par pricing model, posed a threat to its signature-based products, both debit and credit, and the interchange revenue that supported those products. According to Andersen Consulting, Visa's consultant, "there [was] a clear danger that Visa Debit and Credit transactions [would] be preempted by the lower regional [PIN debit] mark. This is ... [a] strong threat to Visa interchange income."¹⁶ The interchange income that Visa thought was at risk was quite large — Andersen projected an annual reduction of \$813 million.¹⁷

13. As a result, Visa launched strategies to increase the interchange charged by the PIN debit networks and to push the debit market away from PIN debit and toward signature

¹⁴ **Attachment 7** (Financial Impact of Direct Debit Evolution, Product Development and Marketing Committee, Board of Directors, Visa U.S.A., Andersen Consulting, June 1990) at AND1018585.

¹⁵ **Attachment 13** (Visa U.S.A. Inc. Special Meeting of the Board of Directors, Apr. 19, 1991) at 0024983.

¹⁶ **Attachment 14** (Visa U.S.A. Debit Services Strategy, June 1990) at AND1018571.

¹⁷ **Attachment 7** (Financial Impact of Direct Debit Evolution, Product Development and Marketing Committee, Board of Directors, Visa U.S.A., Andersen Consulting, June 1990) at AND1018611, AND1018616.

debit, notwithstanding its relative low levels of security. To make this happen, Visa leveraged its “honor all cards” (“HAC”) rules that forced merchants accepting ubiquitous Visa credit card transactions to accept Visa signature debit card transactions as well. The HAC rules ensured that merchants accepted signature debit transactions at credit card-like interchange rates: no merchant could refuse to accept Visa (or MasterCard) signature debit cards if it meant that they could no longer accept Visa (or MasterCard) credit cards as well.¹⁸ And without the high interchange enabled by these rules, banks would not have had the incentive to issue signature debit and limit the growth of PIN debit.¹⁹

14. Spurred by the credit card-style interchange associated with signature debit, after years of languishing growth, Visa’s strategy began to motivate banks to issue the product in the early 1990s. As issuance of signature debit took hold, banks that had previously issued debit cards with the regional PIN debit marks on the front of the cards relegated those marks to the back of the cards, while simultaneously adding the Visa (or, in some cases, MasterCard) logo to the front of the cards.²⁰ Thus, cards that once only had PIN debit functionality, now had both signature and PIN debit functionality, and the PIN debit component was deliberately obscured.

15. The success of Visa’s signature debit-oriented strategy forced MasterCard to reverse course and parrot Visa, dealing another major blow to the growth of PIN debit. In March

¹⁸ See, e.g., **Attachment 15** (Deposition testimony of Stephen Hunter, Wal-Mart, Mar. 14, 2000) at 75-76 (testifying that because there is no ability for Wal-Mart to choose to accept credit without offline debit, Wal-Mart is forced to accept offline debit cards: “The alternative is that we don’t take credit, which is not a reasonable alternative.”).

¹⁹ See, e.g., **Attachment 16** (MasterCard memorandum re: U.S. Debit Strategy, Oct. 20, 1994) at MD1287-0228 (“Given interchange fee and the broad acceptance of MasterCard and Visa, a bank can issue the [offline] debit product and generate significant incremental revenue virtually overnight. This trend has not benefited MasterCard. Initially having been positioned behind Maestro, we are now playing catch-up in off-line debit.”).

²⁰ See, e.g., **Attachment 17** (Deposition testimony of Stephen Cole, Cash Station, Dec. 2, 1999) at 35-36 (the “vast majority” of financial institutions issuing Cash Station cards issued them with the Cash Station logo on the front of the cards, until the popularity of Visa’s and MasterCard’s signature debit cards increased, “at which time in most cases the [Cash Station] logo was reverted to the back of the card”).

1994, MasterCard installed Gene Lockhart as CEO to replace Pete Hart, who had been committed to pushing Maestro PIN debit as MasterCard's lead debit strategy. After that time, MasterCard followed Visa's lead and pushed signature debit as its lead product, forcing merchants with its HAC rule to accept MasterCard signature debit transactions at the same rates they paid for MasterCard credit card transactions. In fact, these rates were the highest interchange rates at the time in the debit market. After 1994, MasterCard allowed Maestro to languish in the United States where it basically had no appreciable market share until very recently.²¹

16. With both Visa and MasterCard using HAC rules to support high signature debit interchange to compete for bank issuance, banks increasingly issued signature debit and took steps to limit the growth of PIN debit. Bank issuance of signature debit exploded between 1993 and 1998,²² and many banks took steps to suppress PIN debit.²³ For example, some banks charged consumers a fee for PIN debit and not signature debit.²⁴ These practices have continued

²¹ **Attachment 18** (General Purpose Debit Card Market Purchase Volume Shares, 1995–2006) (reflecting a zero PIN debit market share (in terms of volume) for Maestro from 1995–2006); *see also* Steven C. Salop *et al.*, *Economic Analysis of Debit Card Regulation Under Section 920*, Oct. 27, 2010, at Exhibit 3 (PIN Debit Networks' Share of Debit Market - 2009) (indicating a 2.7 percent PIN debit share for Maestro in 2009).

²² According to Visa, between 1994 and 1998, signature debit's share of the debit market increased 25 percent (from 41 to 66 percent) while PIN debit's share decreased 25 percent (from 59 to 34 percent). **Attachment 19** (Commerce Bank Deposit Access Products Update, Visa, July 15, 1999) at 1618020.

²³ Results of a 2002 survey "suggest[ed] that banks are in fact stepping up their promotions of signature-based debit and/or instituting penalty fees on Pin-based debit. Fifteen of the 50 debit card issuers to whom we spoke, or 30%, had some policy in place to discourage Pin-based debit." **Attachment 20** ("Concord EFS, Inc., Reducing Price Target from \$39 to \$30 Based on Debit Card Survey Findings," JMP Securities, July 24, 2002) at 2. Another 2002 survey of the-then top 250 debit card issuers found that approximately 20 percent "have instituted punitive policies that charge consumers a fee for PIN-entry" or other incentive programs to steer customers to signature debit). **Attachment 21** ("Sign on the Dotted Line: Are PIN-Debit Expectations Too High?," Jefferies & Company, June 4, 2002) at 4.

²⁴ *See, e.g.*, **Attachment 22** (PULSE Debit Issuer Survey: Cardholder Fees & Industry Outlook, Dove Consulting, Aug. 2, 2002) at 1, 7 (finding that 26 percent of the 50 financial institutions surveyed charge a PIN debit-only penalty fee, averaging \$0.50). According to Dove, imposing such penalties reduced online debit usage by 40 percent. *Id.* at 19. *See also* **Attachment 23** ("NYPIRG Survey Finds ATMs are Always Taking Money From Consumers," New York Public Interest Research Group, Apr. 9, 2002) at 3 (finding that 57 percent of the approximately 50 banks surveyed charge PIN debit penalty fees, averaging \$0.89); **Attachment 24** ("Debit-card

to this day. To cite two recent examples, Chevy Chase Bank (which was recently purchased by Capital One) charges cardholders \$0.50 for PIN debit transactions, whereas signature debit transactions are free.²⁵ Similarly, Connecticut-based Higher One, which specializes in financial products for students, charges students \$0.50 for PIN debit transactions, while charging nothing for signature debit transactions.²⁶

17. Banks also use special promotions to encourage signature debit at the expense of PIN debit.²⁷ They adopt rewards programs such as air miles, cash rebates and prize sweepstakes for which only signature debit transactions qualify, and PIN debit is excluded (*e.g.*, “Skip the PIN, Sign and Win!”²⁸). For example, Wells Fargo, one of the largest debit issuers in the United States, provides bonus rewards points on “Check Card” purchases, but only if the transaction is completed via signature debit.²⁹ Regions Bank similarly offers cardholders a statement credit if

users Stuck with new PIN fees,” ConsumerReports.org, June 2002) at 1 (finding that 5 of the then-10 largest debit card issuers charge PIN debit penalty fees, ranging from \$0.25 to \$1.50); **Attachment 25** (“Issuers Add PIN Fee In Hopes Of Getting More Signature Use,” ATM & Debit News, May 9, 2002) (finding that 11 of the 27 financial institutions surveyed charge PIN debit penalty fees, ranging from \$0.25 to \$1.50).

²⁵ **Attachment 26** (Chevy Chase Bank Schedule of Fees – Personal Accounts).

²⁶ **Attachment 27** (Higher One website, “Additional Fee-Based Services,” <https://ivcone.higheroneaccount.com/info/outadditionalfees.jsp>) (“Instead of entering your Personal Identification Number (PIN) at checkout, choose ‘credit’ and sign the receipt to avoid the PIN fee.”).

²⁷ Dove Consulting’s 2002 survey found that 56 percent of the banks it surveyed sponsor offline-only promotions. **Attachment 22** (PULSE Debit Issuer Survey: Cardholder Fees & Industry Outlook, Dove Consulting, Aug. 2, 2002) at 24.

²⁸ **Attachment 28** (“Commerce Bank Launches Skip the PIN, Sign and Win Sweepstakes for Third Consecutive Year,” Business Wire, Apr. 9, 2002); *see also* **Attachment 29** (CDC Federal Credit Union website, “Skip the Pin and win \$500 cash!”, http://www.cdcfcu.com/asp/general_19.asp) (“From now until October 31, 2010, use your CDC FCU VISA debit card to make purchases, select ‘credit’ and sign to authenticate. If you are immediately prompted for your PIN, select ‘cancel’ and choose ‘credit’ to sign for your purchase. By doing this, you will be automatically entered into our Skip the Pin and Win contest!”); **Attachment 30** (First National Bank Texas website, “Skip the Pin Sign & Win Sweepstakes . . .,” <http://www.1stnb.com/en/specials/sweepstakes/sweepswinners.php>).

²⁹ **Attachment 31** (Wells Fargo website, “How do Wells Fargo Check Cards work?,” <https://www.wellsfargo.com/checkcard/manage/howitworks>) (“You must press the ‘Credit’ button and sign for your purchases if you wish to earn rewards points in one of the optional Rewards programs.”). *See also* **Attachment 32** (JPMorgan Chase website, “Chase Debit Cards – Chase Continental Airlines Debit Card,” https://www.chase.com/index.jsp?pg_name=ccpmapp/individuals/debit_cards/page/continental_airlines) (“Qualifying purchases [for Chase Continental Airlines miles] include all debit card purchases made without using a PIN. . . . If asked ‘Debit or Credit,’ always select ‘CREDIT’ and sign for the purchase.”); **Attachment 33** (US Bank

they make a certain number of signature debit transactions.³⁰ Many banks instruct cardholders to always sign for their debit purchases or press the “Credit” button to make a signature debit transaction at the merchant terminal.³¹

18. JPMorgan Chase recently went so far as to encourage consumers (in a customer mailer) to avoid PIN debit because “you won’t have to enter your PIN in public,”³² even though the fraud associated with shoulder surfing (when someone steals your PIN by looking over your shoulder) pales in comparison to the fraud risks associated with signature debit. John Fennell, an executive of New York Community Bank, explained the \$1.50 charge assessed by his bank for each PIN debit transaction: “We are trying to encourage people to use debit cards the way they are supposed to be used, not with a PIN We want everybody to use them as credit cards.”³³

19. Signature debit also has managed to completely monopolize Internet transactions, even though its lack of security over the Internet creates serious issues, and even though 79 percent of consumers surveyed in 2009 by Javelin Strategy & Research said that they would feel

website, “Check Card FAQs,” <http://www.usbank.com/en/checkcards/questions.cfm>) (“Only non-PIN transactions earn rewards and are protected by the U.S. Bank Zero Liability Policy.”); **Attachment 34** (USAA Bank website, “Free Checking,” https://www.usaa.com/inet/ent_utils/McStaticPages?key=no_fee_checking_main) (“Select ‘credit’ at checkout; PIN-based purchases do not earn points.”); **Attachment 35** (Citibank website, “Citibank®/AAdvantage® Debit Card,” <https://online.citibank.com/US/JRS/pands/detail.do?ID=AAdvantageCard>) (“To earn AAdvantage® miles, you must press Credit when making purchases.”).

³⁰ **Attachment 36** (Regions Bank mailer).

³¹ **Attachment 37** (Bank Atlantic website, “Debit/ATM Card FAQs,” <http://www.bankatlantic.com/FAQ/Debit-ATMCardFAQs/default.html#q07>) (“At merchants that accept Debit MasterCard, you should always press ‘CREDIT’.”); **Attachment 38** (B&K Bank website, “Debit & Credit Cards,” <https://www.bkbank.com/personal-cards.htm>) (“Always select ‘CREDIT’ and SIGN: It’s the best practice for debit use.”); **Attachment 39** (First American Bank website, “Debit/ATM Card FAQs,” <https://www.fabt.com/FAQ-debit-atm.html#6>) (“You should always press ‘CREDIT’ at any merchant that accepts our Visa Debit card.”).

³² **Attachment 40** (“Counterintuitive Pitch for Higher-Fee Debit Category: JPMorgan Chase tells customers signatures are safer than PINs,” AMERICAN BANKER, Apr. 21, 2010).

³³ **Attachment 41** (Heike Wipperfurth, “Banks Sock NYers with Debit Fees: More Institutions Quietly Charge for PIN-based Buys; No End in Sight,” CRAIN’S N.Y. BUS., May 20, 2002). *See also* **Attachment 42** (First Union CheckCard Two Year Risk Assessment) at 6 (“First Union is combating the growth of on-line [debit] in several ways ... The strategy is to build a preference for always signing the receipt versus entering a PIN.”).

more comfortable using a PIN for their Internet purchases.³⁴ In the past decade, several attempts have been made to bring PIN debit to the Internet in the U.S., and none of them have gained traction because the banks have wanted to protect the card-not-present interchange rates they get from signature debit transactions over the web. Examples include Acculynk, which is currently struggling to get traction, HomeATM, and PIN-equivalent systems such as NACHA's Secure Vault Payments, which redirect the consumer's browser to his/her online bank for authentication and authorization.³⁵ After zero liability was implemented in 2000,³⁶ consumers could repudiate Internet transactions with impunity and shift the cost of those transactions — “friendly fraud” to the industry — onto the merchant. In fact, some estimates assert that as many as 66 percent of the chargebacks that merchants suffer for card-not-present transactions involve situations in which the transaction was valid and properly processed, but was either made by a family member or friend without permission or knowledge, or was simply rejected by the cardholder who changed his/her mind or who set out to game the system. Based on zero liability, signature debit has been marketed to consumers as having better “protection” than PIN debit, where the cardholder is responsible for the transaction (except in cases of merchant fraud or non-performance).³⁷

³⁴ **Attachment 43** (“Pulse Introduces PIN Debit for E-commerce Transactions,” News Release, July 14, 2010, <http://www.acculynk.com/us/press/PULSE%20Internet%20PIN%20Debit%20News%20Release.pdf>).

³⁵ The Interac PIN debit system in Canada uses a process similar to Secure Vault to facilitate direct debit transactions over the Internet.

³⁶ Visa and MasterCard initially adopted limitations on consumer liability in 1997, whereby consumer responsibility for losses related to offline debit fraud was zero only if the consumer reported the loss within two days of discovery, and \$50 if the loss was reported after two days. Beginning in 2000, Visa and MasterCard changed that liability to zero, regardless of when the consumer reported the fraud.

³⁷ Regulation E, 12 CFR 205.6, governs cardholder liability on PIN-based debit transactions.

20. With PIN-based alternatives suppressed, Visa reported in 2005 that Visa signature debit card transactions exceeded Visa credit card transactions over the Internet.³⁸

21. These tactics have succeeded over the years in limiting the growth of PIN debit. In 1993, when Visa and MasterCard began promoting their signature debit programs, PIN debit accounted for roughly 60 percent of all debit transactions. By 1998, signature debit accounted for roughly 60 percent of debit transactions, almost precisely the mirror image of five years earlier.³⁹ And in 2001, Visa had a 78 percent share of the signature debit segment, and a 56 percent share of the market as a whole.⁴⁰ Today, signature debit is still the leading form of debit in the United States, and Visa's share of debit is now 66 percent.⁴¹

E. The Convergence of Signature and PIN Debit Interchange Rates

22. Visa also set out to drive up PIN debit interchange under the higher signature debit interchange umbrella that prevailed. First, in 1991, Visa bought one of the leading PIN debit networks, Interlink, which at the time accounted for almost 60 percent of all PIN debit transactions, and about 31 percent of all point of sale debit transactions.⁴² Immediately upon making that purchase, Visa increased Interlink debit interchange from at-par to \$0.45. This

³⁸ **Attachment 44** (“Visa Reports That Debit Transactions Exceed Credit Volume On The Web,” ATM & Debit News, July 14, 2005).

³⁹ See Steven C. Salop *et al.*, *Economic Analysis of Debit Card Regulation Under Section 920*, Oct. 27, 2010, at Exhibit 6 (Relative Share of PIN and Signature Debit - 1991–2009). Also, in 1998, Visa introduced a new product, Visa Check Card II, which provided both PIN debit and signature debit options. While issuance of the card was minimal, and has all but disappeared today, it charged exorbitant interchange fees. This high interchange led to significant price increases by the regional PIN debit networks. As one Visa strategy document made clear, this is exactly what Visa planned: “Pricing to protect ‘the floor.’ Defending value of on-line transaction. ... Even if product is never successful, ‘you have earned your spurs’ (regional networks will increase cost).” **Attachment 45** (Visa handwritten notes) at 1625777. These PIN debit price increases diminished merchants’ incentives to install PIN pads, thus helping to further entrench signature debit.

⁴⁰ **Attachment 18** (General Purpose Debit Card Market Purchase Volume Shares, 1995–2006).

⁴¹ See Steven C. Salop *et al.*, *Economic Analysis of Debit Card Regulation Under Section 920*, Oct. 27, 2010, at Exhibit 2 (Debit Card Market Shares Based on Purchase Transactions and Dollar Volumes - 2009) (In 2009, signature debit accounted for 67 percent of total debit transactions, while Visa debit (signature and Interlink combined) accounted for 66 percent of total debit transactions).

⁴² THE NILSON REPORT (ISSUE 523), May 1992, at 4-5; THE NILSON REPORT (ISSUE 525), June 1992, at 8.

change was unprecedented; at the time, all of the competing PIN debit networks either were at par or had reverse interchange.⁴³

23. Throughout the 1990s, Visa kept Interlink's rates higher than those of any other PIN debit network.⁴⁴ Then, beginning in 1999, Visa began raising those rates even higher to close the gap between PIN and signature debit rates. For small non-supermarkets,⁴⁵ Visa raised Interlink rates in 1999, 2002, 2005, 2009 and 2010. In each instance, the price increase rendered Interlink as the highest-priced PIN debit network, and the 2010 increase converged Interlink with signature debit rates. Visa raised the Interlink rates charged to the largest non-supermarket merchants in 1999, 2005 and 2010, and each increase rendered Interlink the highest-priced PIN debit network. The same can be said about Interlink's supermarket rates. For small supermarkets, Interlink raised its rates in 1999, 2002, 2005, 2008 and 2010. Each increase left Interlink as the highest-priced PIN debit network, and the 2010 increase converged Interlink and signature debit rates. Interlink rates charged to the largest supermarkets were increased in 1999, 2002, 2005 and 2010. Interlink's rates charged to the largest supermarkets are currently higher than comparable rates set by the competing PIN debit networks.⁴⁶

24. Competing PIN debit networks raised their interchange rates under the umbrella created by Visa in order to retain the business of issuers. Merchants had little choice but to

⁴³ **Attachment 46** (PIN Debit Network Interchange Fees, 1992 to 1999).

⁴⁴ **Attachment 47** (Visa document entitled "POS Debit Market 1992–2000") at 1571729 (referencing "Interlink's higher interchange" relative to "Non-Interlink" PIN debit networks for 1991–1997).

⁴⁵ According to Interlink's 2010 interchange fee schedule, small merchants are defined as any merchant whose Interlink volume was less than 17.5 million transactions or \$650 million in the 12-month period ending September 30, 2009. These small merchants pay the Interlink "Standard" interchange fee rate. According to the same fee schedule, the largest merchants are defined as any merchant whose Interlink volume was greater than 88 million transactions and \$4 billion in the 12-month period ending September 30, 2009. These largest merchants pay the Interlink "Tier 1" interchange fee rate.

⁴⁶ See Steven C. Salop *et al.*, *Economic Analysis of Debit Card Regulation Under Section 920*, Oct. 27, 2010, at Exhibit 1a-1d (Interchange Fee For Selected Debit Networks, 1990–2010).

accept these price increases because if they refused to accept Interlink or its competitors in the PIN debit segment, the transaction would default to the more expensive signature debit product.⁴⁷ These price increases resulted in a market-wide effective interchange increase of 234 percent between 1998 and 2006.⁴⁸ And since 2006, PIN debit interchange fees have continued to increase dramatically. By 2010, for many retail categories, signature and PIN debit interchange rates were virtually the same.⁴⁹

25. Visa was able to drive this movement to increase PIN debit interchange rates, in large part, because of its ability to enter into exclusive and near-exclusive issuance deals with banks that resulted in a large percentage of debit cards in the marketplace bearing Interlink as the only PIN debit option. By 2004, Visa had exclusive (or near-exclusive) debit deals with virtually all of the major debit issuing banks, totaling hundreds of banks.⁵⁰ These deals both expressly obligated banks to issue all of their signature debit cards as Visa cards and effectively obligated banks to route all or most of their PIN debit transactions over Visa's Interlink network. To entice banks to issue Interlink on an exclusive (or near-exclusive) basis, Visa offered banks large volume-based rebates from the fees and assessments that these issuers paid Visa as well as substantial upfront "marketing" payments.

⁴⁷ In September 2001, a handful of merchants, including Wal-Mart, Publix Supermarkets, Walgreens and Racetrac Petroleum, publicly announced their intention to drop Interlink to counter a price increase it was planning to implement the following month. As a result, Interlink delayed its price increase until March 2002. This is the only example of merchant resistance to the huge increases in online debit interchange rates in the past two decades that I can recall. And all of those merchants continue to accept Interlink, notwithstanding its ongoing rate increases.

⁴⁸ **Attachment 48** (Weighted Average PIN Debit Interchange Fees, 1998–2006).

⁴⁹ See Steven C. Salop *et al.*, *Economic Analysis of Debit Card Regulation Under Section 920*, Oct. 27, 2010, at Exhibit 1a-1d (Interchange Fee For Selected Debit Networks, 1990–2010).

⁵⁰ **Attachment 49** (*United States v. Visa U.S.A. Inc.*, No. 98 Civ. 7076 (BSJ), 2007 WL 1741885, at *1 (S.D.N.Y. June 15, 2007)) ("By early 2004, Visa [who at the time commanded 80% of the offline debit market] had renewed long-term contracts with most of its member banks, essentially locking up 89% of the volume of its top 100 debit issuers."). Many of these deals were broad-based dedication agreements that covered both credit cards and debit cards.

26. This strategy changed the debit market between 2001 and 2006. During this time frame, Visa entered into exclusive or near-exclusive deals with numerous large issuers.⁵¹ In 2001, Interlink's share of PIN debit was 10 percent, smaller than STAR's 55 percent.⁵² By 2006, after Visa had entered into exclusive or quasi-exclusive deals with a number of major banks, Interlink's 39-percent share exceeded STAR's 32-percent share.⁵³ At the same time, with Interlink as the leading PIN debit network (accounting for nearly 40 percent of PIN debit volume), Visa's share of the total debit market had increased to 63 percent.⁵⁴

27. The proliferation of deals that resulted in Interlink being the exclusive or primary PIN debit network option on many debit cards has enhanced and cemented Visa's ability to increase PIN debit pricing without losing merchant acceptance. With other PIN debit marks removed, merchants have little or no choice but to accept whatever price Interlink forces them to pay. They cannot route transactions to a cheaper PIN debit network. And if they reject Interlink, they will merely move the transaction to Visa's even more expensive signature debit network.

28. Today, Interlink is by far the leading PIN debit network.⁵⁵ The extent to which it dominates the market is apparent from the merchant data that has been collected for this submission. That data shows that large merchants with sophisticated programs that route PIN transactions away from Interlink in virtually all cases still receive approximately 42 percent of their debit volume as Interlink transactions. Given the sophistication of this steering program,

⁵¹ **Attachment 49** (*United States v. Visa U.S.A. Inc.*, 2007 WL 1741885) at *1.

⁵² **Attachment 18** (General Purpose Debit Card Market Purchase Volume Shares, 1995–2006).

⁵³ *Id.*

⁵⁴ *Id.*

⁵⁵ See Steven C. Salop *et al.*, *Economic Analysis of Debit Card Regulation Under Section 920*, Oct. 27, 2010, at Exhibit 3 (PIN Debit Networks' Share of Debit Market - 2009) (indicating that Interlink's 13.8 percent share (in terms of transactions) of total debit in 2009 was greater than the combined debit share of the next three-largest PIN debit networks (STAR – 6.1 percent, PULSE – 4.2 percent, and Maestro – 2.4 percent)).

this result can be treated as a proxy for the percentage of PIN-capable debit cards that bear only Interlink functionality. This shows that hundreds of millions of debit cards in the market today have no PIN debit alternative to Interlink. As such, roughly 56 percent of Visa signature debit cards bear only Interlink as the PIN debit option on the card.⁵⁶

III. DISCUSSION OF INDUSTRY FACTS RELEVANT TO RULEMAKINGS

A. Banks Will Continue to Issue Debit Cards in a Mature Market Without Interchange

i. Banks Make Money on Debit Cards Without Interchange

29. Debit cards are a core convenience that banks provide to consumers. Many bankers view the debit card as an access device with the demand deposit account (“DDA”) being the true product.⁵⁷ Without interchange, debit cards provide numerous benefits to banks that will continue to justify their issuance post-regulation. These benefits include: (i) displacing more costly cash and check transactions;⁵⁸ (ii) motivating cardholders to maintain greater balances, which banks can then lend;⁵⁹ and (iii) helping the bank to cross-sell other lucrative services such

⁵⁶ It is also worth noting that approximately 13 percent of debit cards bear only PIN debit functionality and 7 percent are signature-only, with the latter cards concentrated in the Midwest, particularly Minnesota.

⁵⁷ See, e.g., **Attachment 17** (Deposition testimony of Stephen Cole, Cash Station, Dec. 2, 1999) at 159 (Financial institutions view “[t]he credit card [as] a product unto itself; a debit card is generally not viewed that way. It is an access device to another set of products”).

⁵⁸ **Attachment 22** (PULSE Debit Issuer Survey: Cardholder Fees & Industry Outlook, Dove Consulting, Aug. 2, 2002) at 27 (“Our philosophy around PIN debit is that, even without making money off of it, it saves us money because it’s one less check that we need to process.”); **Attachment 50** (Deposition testimony of Dale Dooley, Shazam, Inc., Sept. 22, 1999) at 85-86 (testifying that from the beginning, banks wanted to utilize online debit cards to eliminate the expense of paper checks, *i.e.*, “to begin working towards an electronic delivery system to eliminate the need to process paper and courier those checks around”); **Attachment 51** (Visa Deposit Access Products, Nov. 1995) at 0740771 (“shifting even only a small percentage of these cash and check payments to deposit access cards adds up to a very large opportunity in terms of potential transactions”).

⁵⁹ **Attachment 5** (Deposition testimony of Arthur Kranzley, MasterCard, Feb. 22, 2000) at 77-78 (testifying that the prevailing view of U.S. banks in the early 1990s was that online debit would increase “the revenues associated with the account” by encouraging account retention, attracting new accounts, increasing account usage, and motivating consumers to maintain higher checking account balances).

as credit cards, mortgages and home equity lines of credit.⁶⁰ It is worth noting that DDAs constitute a major portion of the profitability in retail banking, with some consultants estimating that 87-90 percent of bank profits are derived from this core relationship.⁶¹

30. Moreover, debit cards enhance the “stickiness” of the cardholder’s relationship with his or her bank. As Visa stated in a circular on its debit program, debit cards “[s]trengthen the checking account relationship ... [by] enhanc[ing] the value of checking account services by building customer loyalty and protecting core deposits.”⁶² Once consumers use their debit cards with regularity, the frequent interactions with their banks open up cross-selling opportunities that dramatically reduce the typically-high cost (*e.g.*, \$125 for credit cards) of acquiring new customers.

31. I anticipate that the banks would argue that interchange in some form is necessary to give them incentives to issue debit cards. This is false and it is belied by statements that bankers and payment card executives have made over the years.⁶³ I have reviewed testimony

⁶⁰ **Attachment 52** (Deposition testimony of John P. Danforth, Ph.D., Visa expert, May 5, 2000) at 332-333 (“[T]he availability of debit cards, off-line debit cards, in [financial institutions’] product arsenal has enhanced their ability to deepen relationships with their customers and to attract new customers ... to give them multiple service offerings and to increase the likelihood that the customer will retain the relationship with that institution over a prolonged period of time. ... I’ve seen instances where bankers have attempted to cross-sell a wide range of services, including mortgage loans, consumer loans, lines of credit, off-line debit cards, brokerage services.”); **Attachment 53** (Visa memorandum from Bill Stewart to Sandy English re: “Merchant Issues Surrounding Debit Cards,” Apr. 25, 1997) at 1153385 (stating that “[t]he debit card is meant to enhance an established relationship with a DDA customer”).

⁶¹ Data from First Manhattan Consulting Group (among drivers of consumer profits, 87 percent derives from core deposits (checking, savings, MMDA, CDs); among drivers of small business profits, 90 percent derives from core deposits); *see also* **Attachment 54** (MasterCard memorandum from Jason L. Rodgers to Brantley Orrell re: “Car Rental Debit Acceptance,” Mar. 3, 1997) at MD1060-0601 (stating that banks will “increase DDA accounts by almost any means. Not to issue a debit card on request would be contrary to their mission.”).

⁶² **Attachment 55** (“The Strength & Growth of Check Cards: A Client Perspective,” Visa Advertising Supplement to American Banker) at 0496044; *see also* **Attachment 5** (Deposition testimony of Arthur Kranzley, MasterCard, Feb. 22, 2000) at 270-271 (“Banks were very interested in building customer loyalty to their deposit accounts[,] in acquiring new customers for their accounts and retaining their customers longer which increases profitability because the longer you retain a customer, the more profitable.”).

⁶³ It is worth noting that even TCF Financial Bank, which has filed a lawsuit complaining about the potential for the regulations to result in “below-cost pricing,” admitted on an analyst call that it will continue to issue debit cards post-regulation regardless of what interchange rates it is permitted under the regulations to recover.

from the public *Visa Check* record and note the following testimony that conflicts with the positions that bankers are taking today:

- “Point of sale debit cards would be issued because, if nothing else, for the reason they were originally issued. They were issued as ATM cards. Again, it’s not about — certainly initially it was, and I believe still primarily remains, that it’s about an access, providing remote access, convenient access to the consumer’s account, not driven primarily by the revenues associated with the card.”⁶⁴
- “Interchange was a component of revenue for [a bank’s] point of sale debit program, but the majority of the profitability was based on the use of the account.”⁶⁵
- “[T]here is more to issuing a product to a customer than just a particular return on a particular product and as I believe I stated earlier, that this added convenience and value to our overall debit card and our DDA account by giving customers access to merchants.”⁶⁶
- “I view the customer relationship, and gaining a greater share of it, as the primary driver of profitability. Therefore, I believe you should view adding functionality to the debit card in the context of what it means to deepen the bank’s relationship with the customer. ... [and] if you want to pump up your profits, do a better job of tying your debit card strategy to your overall retail marketing approach.”⁶⁷

ii. *Debit Cards Displace More Expensive Check and Cash Transactions*

32. Lastly, debit cards replace cash and check transactions that are more costly to the issuer.⁶⁸ For example, a 2002 PULSE issuer survey disclosed that all of the issuers surveyed

⁶⁴ **Attachment 56** (Deposition testimony of Steven VanFleet, MasterCard, Nov. 24, 1999) at 394.

⁶⁵ **Attachment 5** (Deposition testimony of Arthur Kranzley, MasterCard, Feb. 22, 2000) at 272; *see also id.* at 77-78 (testifying that the prevailing view of U.S. banks in the early 1990s was that online debit would increase “the revenues associated with the account” by encouraging account retention, attracting new accounts, increasing account usage, and motivating consumers to maintain higher checking account balances).

⁶⁶ **Attachment 57** (Deposition testimony of Thomas Sladowski, Chase Manhattan Bank, Jan. 28, 2000) at 154.

⁶⁷ **Attachment 58** (Expert Report of Kenneth J. Morrison, Apr. 4, 2000, *In re Visa Check/MasterMoney Antitrust Litigation*, No. 96-CV-5238 (E.D.N.Y.) (J. Gleeson)) at ¶ 29 (citing statement of Robert Hill, Mellon Bank).

⁶⁸ **Attachment 59** (Statement of Russell W. Schrader, Senior Counsel and Vice President, Visa U.S.A. Inc., Hearing on Debit Card Issues, Subcommittee on Financial Institutions and Consumer Credit Committee on Banking and Financial Services, Sept. 24 1997) at 2 (“Consumers are attracted to Visa debit cards as a replacement for cash and checks.”); **Attachment 60** (Untitled Visa document) at 0468600 (“Check Cards Are Used to Displace Cash and Checks”); **Attachment 61** (Letter from Susan B. Forman, Visa Director of Corporate Communications, to Kristen Strand, May 1, 1997) at 0331563 (“Debit cards are not meant to replace credit cards, but to serve as a convenient and secure new payment alternative to cash and checks.”); **Attachment 62** (S.J. Diamond, “For What it’s Worth:

expressed a preference for debit card transactions over checks.⁶⁹

B. Debit Card Issuer Costs

i. General Costs Versus Authorization, Clearing and Settlement Costs

33. The costs that can be most easily identified for virtually all issuers are the costs of authorizing, clearing and settling debit cards transactions. Authorization is the process of confirming, by electronic message, whether the cardholder has sufficient funds to pay for the purchase. Clearing involves delivering final transaction data that the issuers can post to the cardholders account, and calculating the fees and charges that should apply to issuers and acquirers. Settlement involves the final calculation of the net financial position of issuers and acquirers. With PIN debit, all of this is accomplished in a single message whereas, with signature debit, this process is split into two messages: the first message concerns the authorization and the second clears and settles the transaction.

34. These processing costs are well known in the industry, as processing is the backbone of the industry and the costs have declined significantly over time. Moreover, these costs do not vary significantly by issuer, as significant economies of scale are reached by most of the debit card issuers, particularly those that have more than \$10 billion in assets.

35. The incremental cost of authorizing PIN debit transactions (with automatic clearing and settlement in a single message) was approximately \$0.0033 in 2004.⁷⁰ The incremental cost of authorizing, clearing and settling dual-message signature debit transactions

Debit Cards Pay Off — And Do it Really Fast,” LOS ANGELES TIMES, Apr. 22, 1985) (debit cards are “more ‘cost efficient’ (i.e., cheaper) than tellers or check processing.”).

⁶⁹ **Attachment 22** (PULSE Debit Issuer Survey: Cardholder Fees & Industry Outlook, Dove Consulting, Aug. 2, 2002) at 27.

⁷⁰ First Annapolis Consulting, “STAR CHEK® Direct Product Overview” Prepared for First Data, June 22, 2004, at 25.

was approximately \$0.0136 in 2007.⁷¹ Both sources for these costs refer to other “card processing costs” related to the transactions, but the amounts indicated are likely limited to the pure costs of authorization, clearing and settlement that are experienced by issuers.

36. Other sources corroborate these figures. For example, First Data processes an estimated 55 percent of signature debit transactions in the United States. At its scale, it typically charges larger clients no more than a penny for authorization and no more than slightly over a penny for clearing and settlement. Assuming a gross margin of 30 percent, that would put the marginal cost of a signature debit transaction at \$0.015.

37. The incremental cost of ACH debit also is about \$0.023.⁷²

ii. *The Remaining Costs of Debit Card Issuance Are Subject to Wide Variations in Reporting and Cost Allocations*

38. As noted above, aside from authorization, clearing and settlement, debit card issuers incur the following costs:

- Network connectivity: the costs of connecting to various networks;
- Network fees and assessments: the fees and assessments charged by the networks that issuers participate in;
- Fraud processing and monitoring: the costs of fraud processing and monitoring, including transaction-based risk management and fraud detection expenses associated with fraud monitoring systems, such as neural networks, and risk management expenses such as lost/stolen reporting costs;
- Back-office support: the costs of claims handling, adjustments, disputes and chargeback processing;
- Customer service and card services: the costs of customer support from call centers, and expenses for card issuance, production and fulfillment;

⁷¹ First Annapolis POS Debit Issuer Cost Study Comprehensive Report, Oct. 23, 2007, at 26, 28. This is consistent with the fact that the First Annapolis survey shows that, on a total cost basis, PIN debit costs are 50 percent lower than signature debit costs. *Id.* at 23.

⁷² **Attachment 63** (Global Concepts Inc., “A Prognosis & Prescription for the ACH Business,” NACHA Payments 2006, May 9, 2006) at 10.

- Net losses: the costs of all losses charged off by the bank for fraud, chargebacks and bad “credit” for signature debit issuers; and
- Compliance: the costs of complying with legal and regulatory regimes related to issuers’ programs, including network and PCI DSS compliance.⁷³

39. Some of these costs, including network fees and assessments, can be readily isolated and tracked with some accuracy. Certain other costs are fixed costs, including back-office costs, customer service costs and compliance costs. The remaining costs that issuers typically incur are rife with potential reporting inaccuracies related to cost accounting and allocation systems that vary widely by issuer. And some of them reflect inefficiencies that signature debit issuers, which predominately outsource the processing of these transactions, have been willing to incur, in large part, because of the high interchange and overdraft fees they receive on those programs that have substantially exceeded the excessive costs that some of these programs incur.

40. Fraud processing and monitoring costs, particularly for signature debit issuers, cannot be isolated without a rigorous allocation that differentiates between the costs properly allocable to signature debit versus credit for issuers that issue both products.⁷⁴ These costs vary widely by bank. In this regard, fraud prevention technology, such as neural networks that are used to identify potentially suspicious transactions, normally operate on both signature debit and credit card transactions. Because fraud on credit cards is usually higher than fraud on signature debit cards, this differential must be taken into account with the allocation.⁷⁵ Moreover, these

⁷³ Rewards and marketing support costs are not included in this list.

⁷⁴ Many of the largest debit issuers, including JPMorgan Chase, Bank of America, Wells Fargo and US Bank, issue both credit and debit cards.

⁷⁵ Network connectivity costs for many banks also should be allocated between credit card and signature debit for issuers that issue both and for PIN debit and ATM functionality.

costs can vary considerably by bank, especially because the underwriting decisions of banks vary widely and can influence the need for fraud prevention investments as well as the application of business rules, which are discussed below. As First Annapolis observed in its 2007 study of debit issuer costs, there is “[g]reat variability in both signature and PIN costs ... among the participants.”⁷⁶ Notably, First Annapolis observed that “PIN-POS debit costs are lower than signature debit for every survey participant and by an average of 102%.”⁷⁷

41. As for the inefficiencies that many signature debit issuers incur, signature debit issuers often outsource their processing and pay high fees for that service. Those fees include services connected to account holds and overdrafts (issues created by the float risks of signature debit), as well as practices discussed below that enhance those risks to generate profits via overdraft fees for banks. Moreover, these costs almost certainly include additional services, such as chargebacks and other service costs that are significantly more expensive than those costs are with PIN debit.

42. With PIN debit, issuers usually decline authorization requests if the cardholder has insufficient funds in his or her DDA.

43. With signature debit, however, because those transactions often take 1-3 days to clear and settle for most transactions (as recently as 2005, 77 percent of Visa signature debit transactions took up to 2 or 3 days to complete),⁷⁸ there is an inherent risk that some transactions will result in overdrafts. This risk is enhanced by the fact that cardholders typically do not understand that their accounts are not reduced immediately for signature debit transactions.

⁷⁶ First Annapolis POS Debit Issuer Cost Study Comprehensive Report, Oct. 23, 2007, at 31.

⁷⁷ *Id.*

⁷⁸ **Attachment 64** (Adam Frisch and Stephen Stout, “Visa 101: Overview of a Payments Company,” UBS Investment Research, June 15, 2005) at 50, 52.

44. Some issuers receive training from outsourcers on how to manipulate their DDA debit posting process in order to maximize the potential for obtaining overdraft fees — *e.g.*, by clearing larger transactions such as mortgage payments earlier in the day, or by bunching smaller transactions at the end of the day, leaving cardholders little or no opportunity to replenish their accounts. One top-40 bank (in terms of assets) manipulated its DDA debit posting over a six-month period, increasing overdrafts from 48 percent of total signature debit revenue to more than 66 percent.⁷⁹ FDIC banks generate 41 percent of their overdrafts from debit cards.⁸⁰ Bank of America recently reported that 60 percent of its DDA overdrafts were the result of signature debit activity.⁸¹ I have estimated that overdrafts comprise as much as 50 percent of industry signature debit revenue — in effect as much as interchange. More importantly, studies have shown that bank gross margins on overdrafts are 94 percent.⁸²

45. I have seen statements by banks in public filings about their anticipated interchange post-regulation. From these statements, one can estimate the costs that these banks think they will be permitted to recover as interchange after the regulations go into effect. According to Bank of America's pronouncements, it believes it likely will be able to recover between \$0.10-\$0.18 under the regulations.⁸³ Those costs are obviously not limited to the processing costs associated with authorization, clearing and settlement. They likely include additional costs, including network connections and fees, fraud prevention and risk management

⁷⁹ Signature Debit NSF Analysis, Bank Client of BetterBuyDesign.

⁸⁰ **Attachment 65** (Kathy Chu, "Bank of America to deny debit card overdrafts," USA TODAY, Mar. 10, 2010, http://www.usatoday.com/money/industries/banking/2010-03-10-bankoverdraft10_ST_N.htm).

⁸¹ **Attachment 66** (Andrew Martin, "Bank of America to End Debit Overdraft Fees, THE NEW YORK TIMES, Mar. 9, 2010, <http://www.nytimes.com/2010/03/10/your-money/credit-and-debit-cards/10overdraft.html>).

⁸² According to data from Celent.

⁸³ **Attachment 67** (Bank of America Investor Fact Book, Mid Year 2010, <http://phx.corporate-ir.net/External.File?item=UGFyZW50SUQ9NjI0Mjd8Q2hpbGRJRDR0tMXxUeXBIPtM=&t=1>) at p. 45.

costs, card production and operation costs, DDA posting and NSF decisioning and customer service expenses (mostly related to signature debit chargeback costs). TCF, for its part, predicts that the interchange fee it can recover will be 26 basis points.⁸⁴ Once again, this implies a view that it will recover costs well in excess of authorization, clearing and settlement, including all of the categories that Bank of America apparently believes it will recover.

C. Industry Data on Fraud

i. Merchants Bear a Substantial Portion of the Fraud Costs

46. In a 2010 analysis of fraud in the payments business, Rick Sullivan of the Federal Reserve Bank of Kansas City concluded that issuers bear 59 percent of fraud costs, with merchants picking up the remaining 41 percent.⁸⁵ According to Sullivan's analysis, issuers lost slightly more than \$2 billion in fraud losses in 2006 and merchants lost \$1.4 billion. Notably, this analysis was not limited to debit card fraud, although his appendix provides data sufficient to determine that issuer and merchant fraud losses for *debit card* transactions at the point of sale and over the Internet were about equal in 2006.⁸⁶ While the Sullivan paper provides a good threshold discussion of the issues associated with fraud, it provides only a first step towards understanding the relative burdens that issuers and merchants bear with respect to fraud in the U.S. payment system. As Sullivan acknowledges, because the data are incomplete, the Sullivan

⁸⁴ **Attachment 68** (*TCF National Bank v. Bernanke*, No. 10-4149 (D.S.D. filed Oct. 12, 2010)) at ¶ 101.

⁸⁵ **Attachment 69** (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, Second Quarter 2010, <http://www.kansascityfed.org/Publicat/Econrev/pdf/10q2Sullivan.pdf>) at 112-113.

⁸⁶ According to the appendix, issuers incurred debit card fraud losses of \$365 million, which was comprised of \$336 million in signature debit losses and \$28 million in PIN debit losses. The appendix calculates that merchants incurred debit card fraud losses of \$233 million for card-present transactions, but it does not report a separate measure of debit card fraud losses for card-not-present (*i.e.*, Internet) transactions — rather it reports a combined debit card and credit card fraud loss of \$900 million for card-not-present transactions. If just 16 percent of these combined losses were attributable to signature debit, a metric that is less than signature debit's general percentage of the overall volumes, then merchants and issuers would have incurred identical losses (\$365 million) for debit card transactions in 2006.

paper did not fully account for the massive and soaring costs of PCI DSS compliance and liability for merchants and, therefore, it likely understates the extent to which merchants bear the costs of fraud in the U.S payment system.

47. For card-not-present transactions, merchants — not issuers — bear virtually all of the fraud risk. And for Internet transactions, the level of fraud is significantly higher than in card-present transactions. These two factors, combined with a dramatically increasing share of signature debit volume being transacted over the Internet year after year, mean that merchants are bearing an ever-greater share of debit card fraud. To demonstrate this effect, I have updated the analysis that Rick Sullivan did, using the fraud rates he reports in his appendix along with 2009 debit card transaction volumes and a recent measure of signature debit usage over the Internet. The updated analysis shows that issuer debit card fraud losses were \$499 million in 2009, while merchant debit card fraud losses were significantly higher — \$689 million.⁸⁷ These higher merchant debit card fraud losses do not even include the tremendous amount of PCI DSS costs that merchants have incurred.

48. In 2009, Aite Group interviewed 30 industry risk managers about their fraud and chargebacks, and concluded that total fraud was \$8.6 billion for the U.S.⁸⁸ Other studies (*e.g.*, Mercator Advisory Group and LexisNexis) have much higher estimates of merchant costs⁸⁹ —

⁸⁷ Issuers suffered \$499 million in debit fraud losses (\$457 million in signature debit fraud losses and \$42 million in PIN debit fraud losses), whereas merchants suffered \$689 million in debit fraud losses (\$245 million in card-present and \$395 million in card-not-present signature debit fraud losses, and \$49 million in PIN debit fraud losses). 2009 debit card volumes for this analysis were pulled from The Nilson Report. According to the 2009 Debit Issuer Study, 9 percent of signature debit transaction volume occurred over the Internet in 2008. **Attachment 81** (2009 Debit Issuer Study, Tony Hayes *et al.*, BAI Payments Live, Virtual Conference & Expo, Oct. 21-22, 2009) at 7.

⁸⁸ **Attachment 70** (“Card Fraud in the United States: The Case for Encryption,” Aite Group, LLC, 2010, <http://www.aitegroup.com/Reports/ReportDetail.aspx?recordItemID=625>).

⁸⁹ *See, e.g.*, **Attachment 71** (*Credit Card Issuer Fraud Management*, Report Highlights, Mercator Advisory Group, Dec. 2008, http://www.sas.com/news/analysts/mercator_fraud_1208.pdf) at 7 (Figure 4) (reporting potential U.S. credit card-related fraud losses in 2007 at likely \$16 billion and counting); **Attachment 72** (*2010 LexisNexis True Cost of Fraud Study*, <http://solutions.lexisnexis.com/forms/EM10Retail2010TCFWebinarFall42302>) at 8 (“The true

something Rick Sullivan agrees needs to be studied and understood better, given that “lack of coordination in the payments industry has impeded security improvements.”⁹⁰ I estimate that issuer costs for fraud were \$2.4 billion in 2008.⁹¹ In my view, merchant costs and losses were probably much higher, in large part, because of the soaring costs of PCI DSS compliance and liability.

49. The PCI DSS compliance program imposes enormous costs, and the network fees and fines regarding data breaches impose punitive liabilities on merchants. The PCI DSS standards were created by the five major card brands (Visa, MasterCard, American Express, Discover and JCB) to protect the magnetic stripe system against fraud by imposing stringent data security requirements on all participants in the system, particularly merchants (even though merchants account for well less than half of the data breaches in the system). To accept payment cards, merchants must be certified as “PCI DSS-compliant,” and that requires a certification that the merchant does not store or transmit any payment card information in-the-clear. To obtain the appropriate certification, merchants must hire a Qualified Security Assessor (“QSA”) who assesses whether the merchant’s systems, including its terminals, servers and data centers, are compliant. Merchants must undergo this process and bear additional monitoring, auditing and recertification costs on an annual basis.

50. In addition, if a breach occurs at a merchant location, even if the merchant has been previously deemed compliant, the merchant is immediately determined to be non-compliant and will be exposed to fines and liabilities that likely exceed the reissuance and fraud costs

cost of fraud for retail merchants in 2010 is estimated at approximately \$139 billion.”). In my interview with Rick Sullivan for his paper, we discussed both of these reports and potential flaws in their methodologies.

⁹⁰ **Attachment 69** (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, Second Quarter 2010) at 121.

⁹¹ Of the \$6.89 billion in global fraud reported by The Nilson Report in 2009, I assume 35 percent, or \$2.41 billion, was attributable to the United States. THE NILSON REPORT (ISSUE 951), Dec. 2009.

associated with the breach.⁹² This stems from the fact that if a breach occurs, the merchant must pay all reissuance costs, as well as cover the estimated increase in fraud in the area of the breach — an estimate that likely exceeds the actual increase in fraud.⁹³ Merchants must pay operational costs for issuer replacement of compromised cards at a standard rate of \$1.00 per card.⁹⁴ For large breaches involving more than 10,000 compromised cards, the merchant must pay fines to Visa and MasterCard and fraud reimbursements to issuers that could be in the millions.⁹⁵ To make matters even worse, with some of the merchant breaches of which I am aware, the merchant was using software that had been deemed PCI DSS-compliant by Visa, MasterCard or the processor.

51. Moreover, merchants have no practical ability to challenge any of the subjective determinations of the potential fraud associated with the breach because the networks and issuers have designed the system to avoid any direct contractual relationship with the merchant. Networks can unilaterally assert that certain fraud losses suffered by issuers are possibly the result of a data breach at a given merchant, requiring that merchant to pay substantial fraud-related fines and assessments without the network having to offer any evidence at all supporting the assertion (typically the network bases its determination on certain “algorithms” of its own

⁹² The problems with this system can be highlighted by the fact that after the TJX breach, which was prominently reported, the payment networks and acquirers did not warn merchants about the nature of the attack. To make matters worse, the software that was used by TJX that was exposed to this attack was reported to be in compliance in 2008. Because of these failures, I am aware of large merchants being exposed to breaches, including breaches that were caused by their processor’s failure to become compliant.

⁹³ **Attachment 73** (“Updated Account Data Compromise Recovery (ADCR) Frequently Asked Questions,” Visa, Mar. 19, 2008, http://www.rbsworldpay.us/247/pci_docs/ADCR_FAQs.pdf). If a data breach includes more than 10,000 cards, Visa’s ADCR program will apply and, under this program, merchants are assessed penalties based on the difference between “normal” incidence of fraud in the area in question and the higher fraud that may be caused by the compromised accounts. Visa caps this exposure at 2-5 percent of the merchant’s total Visa volume, a threshold that exposes the merchant to costs that easily could exceed the fraud at issue.

⁹⁴ *Id.* at 6.

⁹⁵ TJX paid an estimated \$250 million for the breach that occurred in its compliant system.

design). Further, under the terms of most merchant contracts, these fines and assessments can be seized from the merchant's escrow account without any advance notice to the merchant. As the CIO of a major retailer testified to Congress last year, the ultimate result is that "retailers pay the costs of the fraudulent transactions, either through chargebacks or credit card company imposed fines and penalties. All of this arises from rules that initially grew from a card monopolist that we have no choice but to do business with, or risk the loss of a large portion of our business."⁹⁶

52. In May 2008, an industry consultant estimated that the cost of just getting merchants "compliant" (which, as noted, means nothing if a breach occurs) might approach \$5.5 billion.⁹⁷

53. This figure represents the upfront costs of compliance, however. A recent survey of 33 members of the Merchant Advisory Group trade association indicated that since PCI DSS compliance began, they had paid a total of \$1.29 billion in PCI DSS costs, including fines and liability assessments to compensate issuers.⁹⁸ Extrapolating this figure across the merchant population, as a whole, results in an estimated \$10 billion in PCI DSS costs to date in terms of compliance and liability expenditures. This is corroborated by estimates derived from merchant data compiled to assist the Board in its rulemakings.⁹⁹ Using a similar methodology, but with a

⁹⁶ **Attachment 74** (Written Testimony of Michael Jones [of Michaels Stores, Inc.] Before the Emerging Threats, Cybersecurity, and Science and Technology Subcommittee, Mar. 31, 2009, <http://www.homeland.house.gov/SiteDocuments/20090331142012-77196.pdf>) at 8.

⁹⁷ **Attachment 75** ("A Deeper Dive into the Cost of PCI Compliance," Payments News, May 16, 2008, <http://www.paymentsnews.com/2008/05/more-on-the-cos.html>).

⁹⁸ **Attachment 76** (POS Terminal Survey Results, Merchant Advisory Group, Oct. 2010) at 9.

⁹⁹ Some of these costs come from investing in interim solutions, such as end-to-end encryption and tokenization to reduce a merchant's exposure to PCI DSS issues. End-to-end encryption involves disguising card credentials via an encrypting algorithm secured by keys that enable only trusted parties (*e.g.*, issuers) to decrypt the transmission to identify and access the transaction account. Typically, this encryption is done on the card, via a computer chip, so that the credentials are never exposed all the way through to the issuer authorization. Tokenization involves the conversion of the card credentials, usually at the moment of the receipt of the credentials, and the secure transposition into an unidentifiable token for subsequent processing. This token is usually passed to a trusted third

more specific assessment of fines and liabilities, the annual cost of PCI DSS compliance and fines will exceed the total bank cost of payment card fraud in the United States.

54. One large merchant that compiled data for this submission spent 41 basis points on PCI DSS compliance per dollar of general purpose card volume from 2007–2009.

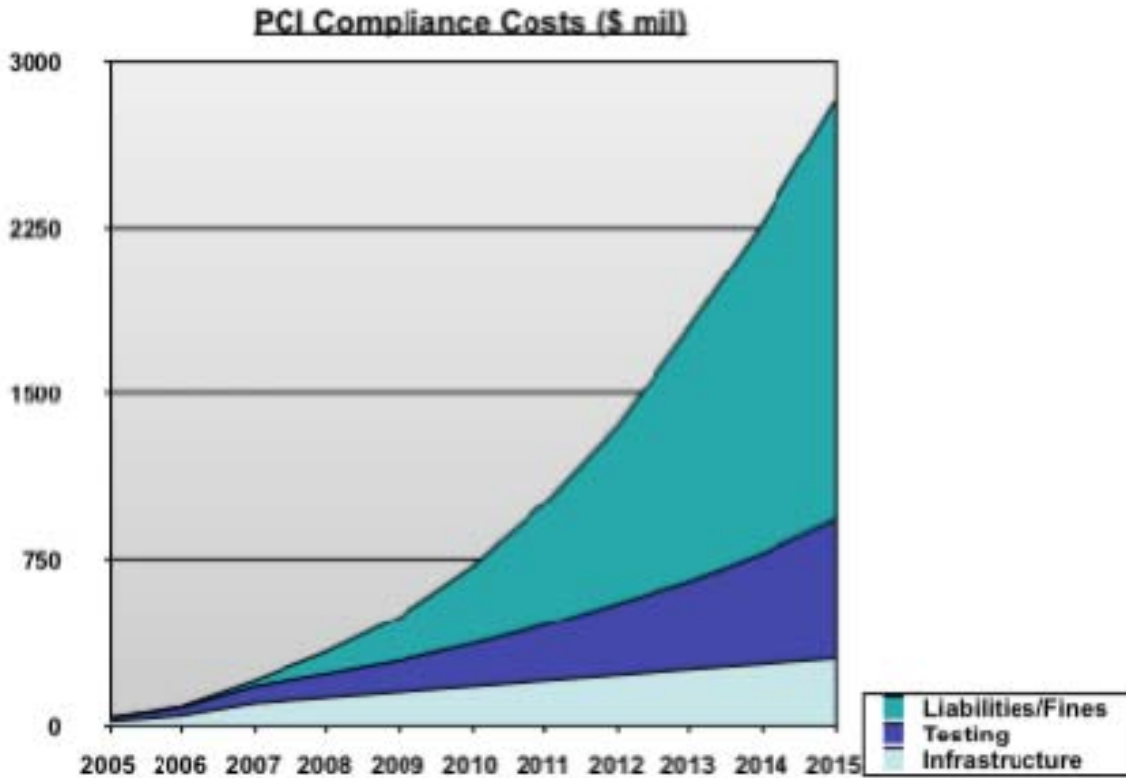
55. If merchants choose to purchase insurance against their exposure to PCI DSS fines, assuming such insurance is even available to them in the market, there are substantial costs and the coverage is not comprehensive and, thus, merchants remain exposed to liability.

56. The PCI DSS system also is contributing to the overall suppression of PIN debit in the United States. I understand that a recent upgrade to the PCI DSS requirements for PIN entry devices (PCI-PED, Version 2.0) is estimated by some sources to impose up to \$20,000 per-store compliance costs on some merchant venues. This cost will likely have a tremendous chilling effect on the installation of PIN pads.

57. If the magnetic stripe system were replaced with an authentication technique that did not require the transmission of cardholder data over the Internet, virtually all of these costs would be unnecessary. In my view, it is particularly punitive to require merchants to absorb the costs of data breaches that are principally caused by issuers' unwillingness to adopt more secure systems.

party that identifies the account and performs the authorization in the normal way — but with no further exposure with the merchant beyond the initial conversion.

58. Below is a chart that shows that the cost of PCI DSS compliance and liabilities will soon exceed the fraud in the system.¹⁰⁰



59. The chargeback system also imposes additional costs on merchants. Before discussing those costs, a word about the limited payment “guarantee” that the networks provide to merchants is in order. To start, that guarantee is virtually non-existent for card-not-present merchants, including Internet, pay-at-the-pump and mail order/telephone order merchants. In fact, the networks charge those merchants for services such as the Address Verification System or the use of ZIP code verification that many fuel dispensers utilize. The “guarantee” is not much better for brick and mortar merchants. To position themselves to re-present (or reverse)

¹⁰⁰ BetterBuyDesign estimates based on industry rates and experiences for Tier 1-4 merchants. (Tier 1 merchants process more than 6 million transactions; Tier 2 (1–6 million); Tier 3 (20,000–1 million); and Tier 4 (below 20,000). Tiers 3 and 4 are self-assessed regimes, whereas Tiers 1 and 2 require external validation.)

chargebacks — which typically require the merchant to reproduce the signed sales slip to prove that an attempt was made at the point of sale to authenticate the cardholder — merchants must invest in cumbersome electronic signature-capture technology. In the alternative, they can implement even more cumbersome back-office procedures to store and maintain signatures on paper slips. Or they can outsource this function to processors. All of this is expensive. On top of that, merchants are charged fees for every chargeback they try to re-present and they pay additional fees if they fail to reverse the chargebacks. Moreover, issuers have shifted the risks associated with defective magnetic stripe cards that need to be manually entered — transactions that are often inherently more fraud-prone — by making it hard for merchants to challenge chargebacks associated with those cards.¹⁰¹ One merchant reported that up to a third of those manually-entered transactions were fraudulent. Notably, merchants cannot reject such transactions at the point of sale without violating Visa’s and MasterCard’s HAC rules.

60. In many cases, the chargeback fees (as much as \$25–\$35 for large merchants, and over \$100 for small Internet merchants) exceed the value of the transaction, eliminating the merchants’ incentives to contest the chargeback.¹⁰² This disincentive is compounded by the 1-percent chargeback threshold that Internet merchants must maintain. To maintain this threshold and avoid onerous fines, such merchants often “eat” 1-2 percent of potential chargebacks. As a result, legitimate transactions are almost certainly turned away. A CyberSource survey reported

¹⁰¹ In those instances, the merchant is required to obtain a manual imprint of the card and store the paper signature, even if the merchant has a signature data capture system. That imposes additional costs and burdens, including burdens associated with the PCI DSS rules that require the merchant to keep the paper signatures locked up and securely maintained.

¹⁰² A First Annapolis acquirer survey found that the percentage of acquirers that charge chargeback fees in excess of \$20 tripled between 2001–2007. **Attachment 77** (Charles Marc Abbey, “The Threat to Price Stability in the Small Merchant Market,” DIGITAL TRANSACTIONS, June 2008, <http://www.digitaltransactions.net/files/0608acq.doc>) at 16.

that Internet merchants spent 0.3 percent of their total sales on fraud protection expenses.¹⁰³

61. The CyberSource survey also reported that Internet merchants challenge only about 50 percent of the chargebacks they receive, and they win less than half of the time when they do.¹⁰⁴

62. Lastly, on top of these costs, one should add the costs of interchange — particularly the costs of signature debit interchange, which merchants likely never would have paid had they had a choice, and which reflect issuers' decisions to push a product that is much more prone to fraud because of the high interchange associated with it. These costs came to approximately \$40 billion in 2007–2009.¹⁰⁵

63. With that background in mind, a complete distillation of merchant expenditures on fraud in the United States must include the following:

- PCI DSS costs — \$10 billion to date (and escalating)¹⁰⁶
- Chargeback costs — likely in excess of \$2 billion over the past three years¹⁰⁷
- Fraud prevention costs
- Customer service costs
- Lost transactions¹⁰⁸

¹⁰³ **Attachment 78** (Jane Adler, “Checking the Chargeback Scourge,” DIGITAL TRANSACTIONS, June 2010, <http://www.digitaltransactions.net/files/DigitalTransactionsJune2010.pdf>) at 34.

¹⁰⁴ *Id.* at 36 (chart).

¹⁰⁵ This estimate is based on the debit volumes reported in The Nilson Report for the 2007–2009 period (Issues 879, 902, 914, 924, 938 and 942), and the average effective interchange fee rates for PIN and signature debit that were identified by debit issuer surveys conducted on behalf of the PULSE/Discover network. **Attachment 79** (Executive Summary, 2010 Debit Issuer Study, Discover) at 14; **Attachment 80** (“An Update on Trends in the Debit Card Market,” Julia S. Cheney, Federal Reserve Bank of Philadelphia, June 2007, <http://www.phil.frb.org/payment-cards-center/publications/discussion-papers/2007/D2007JuneUpdateDebitCardMarketTrends.pdf>) at 6 (citing interchange fee data from the First Annapolis 2007 Debit Issuer Study).

¹⁰⁶ *See supra*, ¶ 53.

¹⁰⁷ *See supra*, n.87.

ii. *Issuers are Best Positioned to Police Fraud*

64. Issuing banks have the most tools at their disposal to combat fraud. There are several reasons for this:

- At the outset, the issuer chooses the authentication technology.
- Issuers also underwrite the issuance decision in the first place, whereas merchants do not have that ability.
- Issuing banks have access to the entire history of a debit card, and of the bank account associated with that card. Therefore, issuing banks are best positioned to see trends like spending patterns on a given card, or with respect to a given account, across a multitude of merchants — rather than just use at a single merchant. Merchants, who only see the environment in which a transaction is made, simply do not have the same depth or breadth of an account relationship from which they can do comprehensive risk assessments when a transaction is made. In fact, in the physical world, merchants can do little more than train clerks to look for forged signatures, an exercise that provides little value and would achieve nothing other than to slow down the point of sale at some expense to merchants. Notably, Visa’s Operating Regulations prohibit merchants from insisting on additional identification at the point of sale if the customer does not want to produce it.¹⁰⁹
- Issuing banks have access to a wider range of cards and bank accounts than merchants. This is especially true for the dozen or so largest issuing banks that account for most of the debit issuance in the United States. Because issuing banks have access to such a wide range of accounts, and a wide range of activity in financial services generally, they can again use their data to look for cardholder and account behaviors and trends that merchants have no ability to track.
- The PCI DSS rules reinforce merchants’ inability to effectively screen against fraud. These rules strictly prohibit merchants from storing any debit (or credit) card account information except as tokenized and/or encrypted. As a result, merchants cannot easily maintain or check databases of suspicious cards that may be associated with fraudulent activity. Issuers are not similarly restricted, and this is another reason why they are much better positioned than merchants to combat fraud.

65. Networks, by comparison, are much less well-positioned than issuers to police fraud. They lack the data and cardholder history that issuers have, and their systems are

¹⁰⁸ As noted, this is particularly an issue for Internet merchants that need to keep their chargebacks below 1 percent to avoid onerous Visa and MasterCard fines. Such merchants often turn away legitimate transactions that are potentially suspicious in order to avoid chargebacks and stay under the thresholds.

¹⁰⁹ If the card is unsigned, the regulations do permit a request for identification.

comparatively rudimentary. And most medium and large-sized banks rely on their own systems to manage fraud.

66. Even though they are best positioned to address fraud, issuers appear to lack motivation or incentives to implement effective remedies. Three examples illustrate the problem. First, the 2007 First Annapolis Debit Issuer Study demonstrates a wide variety of levels of success in combating fraud, but with no particular relationship to the types or amounts of investment.¹¹⁰ This is indicative of the fact that issuers lack strong incentives to police fraud — in large part because of the interchange system that more than makes up for the charge-off expenses to issuers. Second, the CyberSource online fraud surveys consistently show the need for merchants to deploy a growing array of fraud prevention measures year-by-year, and CyberSource rates their effectiveness. Among the least effective of those measures has been the issuer-driven association efforts with 3-D Secure (Verified by Visa and SecureCode) — despite the almost exclusive focus the banking industry has provided to this secondary authentication method. Third, at the FS-ISAC (Financial Services Information Security and Analysis Center) conference in May 2010, a senior security officer at a top-3 bank was heard to say, “banks are really no safer than the average business down the street.” The complication, he later stated, was the extensive use of account credentials and individually-identifying information, which often are transmitted in the clear, but wind up utilized in setting up new accounts.

iii. Signature Versus PIN Debit Fraud

67. Signature debit transactions are much more prone to fraud than are PIN debit transactions. According to one study, for example, the average net loss per card in 2008 was

¹¹⁰ First Annapolis POS Debit Issuer Cost Study Comprehensive Report, Oct. 23, 2007, at 43-46.

\$0.15 for PIN debit and \$1.81 for signature debit.¹¹¹ Between 2008 and 2009, fraud rates increased by 43 percent for signature debit, but only 24 percent for PIN debit.¹¹² According to the Sullivan paper, in 2006, signature debit card fraud losses for issuers were 5.1 basis points of purchase volume compared to less than 1 basis point for PIN debit.¹¹³ In other words, by this measure, signature debit is six times more susceptible to fraud than PIN debit.

iv. *Fraud in the U.S. Payment System Compared to Other Jurisdictions*

68. The Sullivan paper concluded that:

[T]he United States has a higher card fraud loss rate than Australia, France, Spain, and the UK. International differences are due to a number of factors, including underlying card payment technology and security standards. For the United States, important factors that lead to a relatively high fraud loss rate include a comparatively weak approval process for debit and credit card transactions and a highly developed Internet economy.¹¹⁴

D. Visa/MasterCard Parallel Conduct in Interchange & Network Fees

69. Visa and MasterCard have a history of parallel conduct with respect to interchange going back over the past twenty years. From the 1990s, examples include parallel rate increases regarding: (i) supermarket rates in 1994; (ii) automated fuel dispenser rates in 1996; (iii) the lowest supermarket and non-supermarket rates in 1998; and (iv) non-supermarket rates in 1999.¹¹⁵ Since 2000, Visa and MasterCard's lockstep conduct in interchange included

¹¹¹ **Attachment 81** (2009 Debit Issuer Study, Tony Hayes *et al.*, BAI Payments Live, Virtual Conference & Expo, Oct. 21-22, 2009) at 12.

¹¹² **Attachment 79** (Executive Summary, 2010 Debit Issuer Study, Discover) at 25.

¹¹³ **Attachment 69** (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, Second Quarter 2010) at 113 (Table 2). A more recent measure of issuer debit card fraud is reported in the 2010 Debit Issuer Study, which shows that signature debit is over seven times more susceptible to fraud than PIN debit. **Attachment 79** (Executive Summary, 2010 Debit Issuer Study, Discover) at 25.

¹¹⁴ *Id.* at 115.

¹¹⁵ **Attachment 82** sets forth a schedule of Visa and MasterCard interchange rates for 1990–1999. In April 1992, Visa and MasterCard's interchange rates for supermarkets were both 1.0 percent, and lowest rates for non-supermarkets were 1.25 and 1.30 percent, respectively. In April 1994, Visa and MasterCard increased their

continuing their practice of synchronized, biannual (April and October) interchange announcements with extremely similar rates, including the introduction of new tiers for premium cards and rewards cards, as well as tiers specially designed for merchant categories such as quick service restaurants.

70. After MasterCard (in 2006) and Visa (in 2008) went public, the pattern of acting in lockstep on interchange continued unabated. There have been no significant changes to their interchange tiers, as the rate structure has remained intact. In addition, as the schedule below shows, Visa and MasterCard also have synched up their network fees to acquirers (which are passed along to merchants). For example, in April 2009, MasterCard replaced its “Access Fee” of \$0.005 with a larger “Network Access and Brand Usage (‘NABU’) Fee” of \$0.0185. Less than three months later, Visa replaced its Access Fee of \$0.005 with a larger “Authorization Processing Fee” of \$0.0195.¹¹⁶

71. In recent years, particularly since they went public, MasterCard and Visa have added numerous network fees that are ultimately paid by merchants, and constitute another form of compensation to issuers and their networks.

supermarket rates to 1.10 percent. MasterCard increased its lowest rate for non-supermarkets to 1.31 percent in April 1996, and to 1.32 percent in April 1997. In April 1996, Visa and MasterCard initiated a special interchange rate of 1.35 percent plus 5 cents for transactions using automated fuel dispensers. In April 1998, Visa and MasterCard increased their supermarket rates to 1.15 percent, and increased their lowest non-supermarket rates to 1.31 and 1.38 percent, respectively. In April 1999, Visa and MasterCard increased their lowest non-supermarket rates to 1.38 percent plus 5 cents, and 1.36 percent plus 10 cents, respectively. Visa also raised its supermarket rates to 1.20 percent.

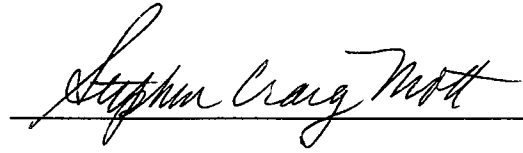
¹¹⁶ **Attachment 83** (“Higher Fees Could be Rainmakers for the Bank Card Networks,” DIGITAL TRANSACTIONS, Mar. 17, 2009, <http://www.digitaltransactions.net/newsstory.cfm?newsid=2118>).

72. Currently, Visa and MasterCard directly (or indirectly via acquirers) charge the following network fees to merchants:¹¹⁷

Network	Network Fee Type	2010	Effective Date
Visa	U.S. Acquirer Service Fee/Assessment Fee	0.11%	7/1/10 (increase)
MasterCard	Acquirer Brand Volume Fee/Assessment Fee	0.11%	4/16/10 (increase)
Visa	Acquirer Authorization Processing Fee	\$0.0195	7/1/09 (new/ replaces \$0.005 Access Fee)
MasterCard	Network Access and Brand Usage (NABU) Fee	\$0.0185	4/17/09 (new/ replaces \$0.005 Access Fee)
Visa	Base II Fee	\$0.0019 ¹	7/1/09 (increase)
MasterCard	Settlement Fee	\$0.0019 ¹	7/1/09 (increase)
Visa	Account Verification Service (AVS) Fee/Zero Dollar Verification Fee	\$0.025	2/1/09 (new)
MasterCard	Address Verification Fee (Card Present/Card-Not-Present)	\$0.005–\$0.0075	10/1/10 (split into two rates)
Visa	International Acquiring Fee (IAF)	0.45% ¹	10/17/09 (new)
MasterCard	Acquirer Program Support Fee	0.55%	10/17/09 (increase)
Visa	International Service Assessment (ISA) Fee	0.40%	4/1/08 (new)
MasterCard	Acquirer Cross-Border Assessment Fee	0.40%–0.80%	10/17/09 (increase)
Visa	Merchant Direct Exchange Connection Fee	\$0.0015–\$0.0045 ¹	
Visa	Risk Identification Fee	\$0.001 ¹	
Visa	Unmatched Authorization Fee/Misuse of Authorization Fee	\$0.045	7/1/09 (new)
Visa	Zero Floor Limit Fee	\$0.10	7/1/09 (new)

¹ 2009 figures (data for 2010 not readily available).

¹¹⁷ This table is compiled from Digital Transactions and other industry publications and processor interviews, and is a sample of acquirer fees, most of which were introduced and/or increased and/or renamed since MasterCard and Visa went public. These types of fees are nearly always passed through to merchants.

A handwritten signature in black ink, reading "Stephen Craig Mott", written in a cursive style. The signature is positioned above a solid horizontal line.

Stephen Craig Mott

New York, NY

October 26, 2010