Fordham Journal of Corporate & Financial Law

Volume 16 | Issue 4 Article 2

2011

Credit Card Fraud: A New Perspective On Tackling An Intransigent Problem

Lydia Segal

Benjamin Ngugi

Jafar Mana

Credit Card Fraud: A New Perspective On Tackling An Intransigent Problem

Cover Page Footnote

Lydia Segal is an Associate Professor of Business Law and Ethics at Suffolk University's Sawyer Business School. With degrees from Harvard Law School and Oxford, her specialty is organizational stewardship and integrity. Her latest book is Battling Corruption in America's Public Schools (Harvard University Press). ** Dr. Benjamin Ngugi, is an Associate Professor in the Information Systems and Operations Management Department at Suffolk University's Sawyer Business School. He received his Ph.D. in Information Systems from New Jersey Institute of Technology and his bachelors degree in Electrical and Electronics Engineering from University of Nairobi, Kenya. He conducts his research in the areas of identity fraud, biometrics, security compliance, e-Health security and technology adoption. He has published his research in journals including Decision Support Systems, International Journal of Information Security and Privacy, and The ACM Journal of Data Quality. + Jafar Mana is a faculty member in the Information Systems and Operations Management Department at Suffolk University's Sawyer Business School. As an entrepreneur, Professor Mana is a cofounder of Analytic Development (ADI) Inc., which provides computer solutions and data analysis to a variety of corporate clients. His research interests are in the areas of product development, modeling and design processes, security and privacy, and knowledge discovery and data mining. 1. The authors wish to thank Professor Jonathan Houghton for his insights on competitive markets and the many business people who shared their insights into the credit card system.

CREDIT CARD FRAUD: A NEW PERSPECTIVE ON TACKLING AN INTRANSIGENT PROBLEM

Lydia Segal[*]
Benjamin Ngugi[**]
Jafar Mana[+]

ABSTRACT[1]

This article offers a new perspective on battling credit card fraud. It departs from a focus on *post factum* liability, which characterizes most legal scholarship and federal legislation on credit card fraud and applies corrective mechanisms only after the damage is done. Instead, this article focuses on preempting credit card fraud by tackling the root causes of the problem: the built-in incentives that

---

[*] Lydia Segal is an Associate Professor of Business Law and Ethics at Suffolk University's Sawyer Business School. With degrees from Harvard Law School and Oxford, her specialty is organizational stewardship and integrity. Her latest book is Battling Corruption in America's Public Schools (Harvard University Press).

[**] Dr. Benjamin Ngugi, is an Associate Professor in the Information Systems and Operations Management Department at Suffolk University's Sawyer Business School. He received his Ph.D. in Information Systems from New Jersey Institute of Technology and his bachelors degree in Electrical and Electronics Engineering from University of Nairobi, Kenya. He conducts his research in the areas of identity fraud, biometrics, security compliance, e-Health security and technology adoption. He has published his research in journals including Decision Support Systems, International Journal of Information Security and Privacy, and The ACM Journal of Data Quality.

[+] Jafar Mana is a faculty member in the Information Systems and Operations Management Department at Suffolk University's Sawyer Business School. As an entrepreneur, Professor Mana is a cofounder of Analytic Development (ADI) Inc., which provides computer solutions and data analysis to a variety of corporate clients. His research interests are in the areas of product development, modeling and design processes, security and privacy, and knowledge discovery and data mining.

1. The authors wish to thank Professor Jonathan Houghton for his insights on competitive markets and the many business people who shared their insights into the credit card system.

keep the credit card industry from fighting fraud on a system-wide basis. This article examines how credit card companies and banks have created a self-interested infrastructure that insulates them from the liabilities and costs of credit card fraud. Contrary to widespread belief, retailers, not card companies or banks, absorb much of the loss caused by thieves who shop with stolen credit cards. Also, credit card companies and banks earn fees from every credit card transaction, including those that are fraudulent. In addressing these problems, this article advocates broad reforms, including legislation that would mandate data security standards for the industry, empower multiple stakeholders to create the new standards, and offer companies incentives to comply by capping bank fees for those that are compliant, while deregulating fees for those that are not compliant.

TABLE OF CONTENTS

INTRODUCTION

Credit card fraud, which is the use of another person's credit card or credit card information for the purpose of stealing, offers criminals one of the fastest routes to riches today. The windfalls, which can reach into the millions of dollars,[2] have attracted a broad spectrum of criminals, ranging from foreign organized crime groups[3] to local street gangs, such as the Los Angeles Crips.[4]

The problem has reached epidemic proportions. Credit card fraud exceeded $3.2 billion in 2007,[5] which is thirty-five percent higher than in 2003.[6] One expert estimates that as many as "[h]alf of all credit card numbers are in the hands of organized criminals" and that "[h]alf of all computers have some form of malware on them,"[7] or malicious software that infiltrates a computer program, records keystrokes, detects account numbers and credit card data, and sends this data to the hacker without the victim's knowledge.

Credit card fraud can lead to identity theft,[8] the cooption of another

---

2. *See, e.g.*, Randall Stross, *Digital Domain $9 Here, 20 Cents There and a Credit-Card Lawsuit*, N.Y. TIMES, Aug. 22, 2010, at BU3, *available at* http://www.nytimes.com/2010/08/22/business/22digi.html?_r=1&scp=5&sq=credit%20card%20fraud&st=cse.

3. *See* JOSEPH MENN, FATAL SYSTEM ERROR: THE HUNT FOR THE NEW CRIME LORDS WHO ARE BRINGING DOWN THE INTERNET 116 (2010) [hereinafter MENN, FATAL SYSTEM ERROR].

4. *See* Joseph Menn, *Gangs Get into Identity Theft*, L.A. TIMES, Aug. 12, 2008, at C3, *available at* http://articles.latimes.com/2008/aug/12/business/fi-idtheft12.

5. Reed Richardson, *Are You Compliant*, SMALL BUSINESS ONLINE COMMUNITY (Apr. 17, 2008, 8:41 AM), http://smallbusinessonlinecommunity.bankofamerica.com/blogs/merchantServices/2008/04/17/are-you-compliant/.

6. *Id.*

7. Interview by Spencer Michels with Joseph Menn, Reporter, FIN. TIMES (PBS broadcast, Aug. 12, 2010), *available at* http://www.pbs.org/newshour/bb/science/july-dec10/cyber_08-12.html (discussing "malware" and electronic theft of financial information).

8. Although credit card fraud and identity theft are related, the two should be distinguished. Credit card fraud is the unauthorized use of a credit card or credit card information for the purpose of stealing. Identity theft involves using stolen personal information, whether from a credit card account or other source, to impersonate another's identity. Identity thieves can use the stolen data to obtain new credit cards, loans, or lines of credit to purchase goods and services under the victim's name. *See generally* Erin Fonté, *Who Should Pay the Price for Identity Theft?*, 54 FED. LAW. 24,

individual's personal information that is subsequently used to obtain new credit cards or bank accounts in the victim's name, costing the victim time, money, and aggravation, as well as damaging his or her credit history.[9] Credit card fraud can also take a major toll on businesses. One study of 45 mid- to large-sized companies found that cybercrime cost each of them an average of $3.8 million per year.[10] These figures do not include the staggering secondary costs of fraud, which can include a loss in stock value,[11] litigation,[12] and payment for the reissuing of breached credit cards.[13]

A. THE CRUX OF THE PROBLEM

There has been an outpouring of creative ideas on how to curb credit card fraud, including many ideas from legal scholars and federal lawmakers. Few of these, however, focus on what we regard as the crux of the problem: the incentives built into the credit card industry[14] to merely contain credit card fraud at "comfortable" levels rather than to attack it directly on a system-wide level. The credit card companies[15]

26-27 (2007) (discussing various methods of identity theft). Identity theft fraud consists of 4% of credit card fraud. *See* Royal Canadian Mounted Police, *Counterfeiting and Credit Card Fraud*, http://www.rcmp-grc.gc.ca/count-contre/cccf-ccp-eng.htm (last visited Aug. 15, 2010).

9. *See* Kevin M. Gatzlaff & Kathleen A. McCullough, *The Effect of Data Breaches on Shareholder Wealth*, 13 RISK MGMT. & INS. REV. 61, 63 (2010); Anne Borden, *The Cost of Credit Card Fraud*, LAWYERSANDSETTLEMENTS.COM (Apr. 29, 2007), http://www.lawyersandsettlements.com/features/credit-card-fraud.html.

10. PONEMON INST., FIRST ANNUAL COST OF CYBER CRIME STUDY: BENCHMARK STUDY OF U.S. COMPANIES 2 (2010), *available at* http://www.arcsight.com/collateral/whitepapers/Ponemon_Cost_of_Cyber_Crime_study_2010.pdf.

11. *See* Gatzlaff & McCullough, *supra* note 9, at 64, 67.

12. *Id.* at 61.

13. *See Study Quantifies the Heavy Damage of Card Data Breaches*, DIGITALTRANSACTIONS.NET (June 4, 2010), http://www.digitaltransactions.net/newsstory.cfm?newsid=2548 (stating that in 2009 it cost companies $252.7 million to replace over 70 million in compromised cards).

14. The "credit card industry" in this article refers to the parties that play a role in credit card transactions. These include the four major card companies, Visa, MasterCard, American Express, and Discover, see *id.*, as well as the banks that issue and settle card transactions, the payment processors, and the merchants.

15. Although there are four major U.S. credit card companies, *see* DIGITALTRANSACTIONS.NET, *supra* note 13, for the sake of simplicity, the discussion in this article will often focus solely on Visa and MasterCard. This is because Visa dominates the market by far, with MasterCard being the second largest company. As of

and banks have engineered an infrastructure designed for their self-benefit that insulates them from the true costs of credit card fraud, thereby blunting their incentives to vehemently fight fraud.

Few people realize that retailers— not card companies or banks— absorb much of the loss[16] caused by scammers who shop with stolen credit cards.[17] The banks that issue credit cards may appear to pay for fraud because they cover cardholders' unauthorized expenses. In fact, however, they pass many of these losses back to the retailer who sold the goods to the criminal. Further, the card brands[18] and banks collect fees from every credit card transaction, regardless of whether it is fraudulent. The card brands also collect fines from the merchants who are victims of the scam.[19] The upshot is that the card brands, which set the security standards for the industry, prefer to merely patch up their inherently fraud-prone security system rather than push for the adoption of safer payment technologies because that would require a greater investment. Meanwhile, millions of American businesses are vulnerable and credit card fraud continues to increase.[20]

This article argues that the legal scholarship and federal laws overlook this structural perspective. The article, which is divided into five parts, advocates a new federal law that mandates data security standards and strengthens the industry's incentives to comply. Part I surveys the legal literature and pertinent federal legislation and shows how neither systematically addresses the crux of the problem. Part II describes the mechanics of credit card transactions and how the industry officially tackles fraud. Part III explains how the industry's current

---

the end of 2009 in the U.S., there were about 270 million Visa credit cards, about 203 million MasterCard credit cards, 48.9 million American Express credit cards, and 54.4 million Discover credit cards. *See* Ben Woolsey & Matt Schulz, *Credit Card Statistics, Industry Facts, Debt Statistics*, http://www.creditcards.com/credit-card-news/credit-card-industry-facts-personal-debt-statistics-1276.php. In terms of global market share, Visa dominates, with MasterCard coming in second, and American Express a distant third. Visa had 64.79% of the 2009 global market share in terms of volume of purchase transactions. MasterCard had 26.5%; and American Express had 4.57%. *See* Nilson Report, *Largest Payment Card Issuers Worldwide* (2010), http://www.nilsonreport.com/largestissuers/index.htm.

16. The assumption underlying the use of the term "loss" in this article is that the stolen goods will not be recovered, leaving someone else to pay for them.

17. *See* MENN, FATAL SYSTEM ERROR, *supra* note 3, at 115.

18. "Card brands" refer to the credit card companies.

19. *See* MENN, FATAL SYSTEM ERROR, *supra* note 3, at 115.

20. *See infra* Part III B.

approach to data security falls short. Part IV explores the root causes for which the credit card industry is reluctant to aggressively tackle fraud. The article concludes with a wide-range of reform suggestions in Part V.

I. REFORM PROPOSALS SKIRT THE KEY ISSUE ABOUT CREDIT CARD FRAUD

A. THE LEGAL SCHOLARSHIP

Although a plethora of law review articles have been written about credit card fraud and the related area of identity theft, virtually none consider the industry's weak incentives to tackle fraud systematically. Instead, most legal scholars focus on how difficult it is under current law for victims of credit card fraud to win damages against companies whose computer networks were breached. Federal laws, after all, rarely give victims a private right of action against breached companies.[21] Courts have been loath to find breached companies negligent so long as they did the minimum amount that is reasonable to secure data.[22] Judges have been reluctant to give victims standing to force companies to be compliant with industry-wide security policies.[23]

Therefore, many legal scholars approach credit card fraud and related identity theft reform with the idea of strengthening the ability of victims to sue infiltrated companies. For example, De Amond urges the adoption of common law or statutory torts to facilitate the ability of victims to sue breached companies for negligence.[24] Weaver recommends that states give consumers a private right of action to allow them to directly sue infiltrated companies so that they would not have to wait for the government to litigate on their behalf.[25] White proposes the

21. Federal courts have held, for example, that the Gramm-Leach-Bliley Act (discussed later) does not provide a private right of action. *See* Dunmire v. Morgan Stanley DW, Inc., 475 F.3d 956, 960 (2007); *In re* French, 401 B.R. 295, 310 (2009).

22. *See, e.g.*, Guin v. Brazos Higher Educ. Serv., 2006 WL 288483 at *4-5 (D. Minn. 2006) (holding a company that exercised reasonable care in handling personal information did not breach its duty to its customers despite a breach that was caused by one of its employees).

23. *See e.g.*, *In re* TJX Cos. Retail Sec. Breach Litig., 524 F. Supp. 2d 83 (D. Mass. 2007).

24. Elizabeth D. De Amond, *A Dearth of Remedies*, 113 PENN ST. L. REV. 1, 52-53 (2008).

25. Owen Weaver, Note, *A Missed Opportunity to Bolster Consumer Protections in*

recognition of a "negligence per se" cause of action for identity theft victims.[26] Schneider advocates allowing victims to sue breached companies for "personal data exposure," a newly recognized type of injury, even if no tangible harm is realized.[27]

Making it easier for victims to sue would undoubtedly help pressure companies to take security more seriously. However, this approach overlooks that many parties in the credit card industry can shift their fraud losses to merchants and consumers, as discussed in Part IV. As a result, making it easier for victims to litigate may not necessarily translate into better security, at least not to the degree expected.

Other scholars approach credit card fraud and identity theft by urging the adoption of specific anti-fraud technologies.[28] Technology plays a central role in data security but, as criminal tactics continually evolve, it is important that the incentives first change to encourage the industry to select the best technological solutions for itself on a continuing basis. Right now, although a plethora of technological innovations exists, the banks and card companies appear more interested in not "rocking the boat" than in pushing for the best options for all parties.[29] The recommendations in Part V may help to change that.

Yet other scholars call on Congress to pass legislation that would impose threshold requirements on handling confidential data[30] or that

---

Massachusetts: How Massachusetts Residents Are Still Without a Private Right of Action After the TJX Security Breach, 43 NEW ENG. L. REV. 677, 700-03 (2009).

26. Anthony E. White, Comment, *The Recognition of a Negligence Cause of Action for Victims of Identity Theft: Someone Stole My Identity, Now Who Is Going To Pay For It?*, 88 MARQ. L. REV. 847, 866 (2005) (arguing that the burden would then be placed on financial institutions, which are best able to avoid liability, to prove otherwise).

27. Jacob W. Schneider, Note, *Preventing Data Breaches: Alternative Approaches to Deter Negligent Handling of Consumer Data*, 15 B.U. J. SCI. & TECH. L. 279, 291 (2009) (citing KENNETH S. ABRAHAM, THE FORMS AND FUNCTIONS OF TORT LAW 47-48 (3d ed. 2007)) (arguing that, although the idea of potential damages is rare, it is not completely foreign to tort law). Schneider suggests that if a retailer is found to have caused injury, damages awarded to the state should be used to compensate victims of identity theft stemming from that incident. *Id*. at 292.

28. *See, e.g.*, Ian Heller, Note, *How the Internet Has Expanded the Threat of Financial Identity Theft, And What Congress Can Do To Fix the Problem*, 17 KAN. J.L. & PUB. POL'Y 84, 106-08 (2007) (advocating biometrics as one of two proposed alternatives to combat identity theft).

29. *See infra* Part III.

30. Amanda Draper, Comment, *Identity Theft: Plugging the Massive Data Leaks with a Stricter Nationwide Breach-Notification Law*, 40 J. MARSHALL L. REV. 681, 699

would require corporations to draft privacy policies.[31] These are critical first steps. However, threshold requirements need to be specific. Privacy policies need to be compatible with other firms' policies, as security in the financial marketplace is interdependent: if the receiving firm is secure but the sending firm is not, security is meaningless. As importantly, any new law needs to offer companies tangible benefits to become compliant with security requirements, as detailed in Part V.

B. FEDERAL LEGISLATION PERTINENT TO CREDIT CARD FRAUD DOES NOT TACKLE THE REAL PROBLEM

Federal laws also fail to give the credit card industry strong enough incentives to combat credit card fraud on a system-wide basis. Only a few federal laws even require companies to preempt cyber crime. Most pertinent laws tackle credit card fraud and related identity theft by criminalizing these acts, thereby providing for the punishment of the thieves after the fact, rather than requiring the prevention of data breaches beforehand. For example, the Computer Fraud and Abuse Act of 1986 ("CFAA") establishes civil and criminal penalties for unauthorized access to computerized data belonging to financial institutions or the federal government.[32] The Cyber-Security Enhancement Act of 2002[33] ("CSEA") makes it a crime to hack into a computer and enhances the criminal penalties already available under the CFAA.[34] The Identity Theft and Assumption Deterrence Act of 1998 ("ITADA") criminalizes identity theft and provides for the FTC to

(2007). "The new law," Draper writes, should "impose strict requirements on how companies handle their confidential data, such as making it illegal to send out information in the mail or online that contains a person's Social Security number, not allowing companies to share their personal customer data with their affiliates, or placing tighter controls on the granting of credit." *Id*.

31. *See, e.g.*, Robert Sprague & Corey Ciochetti, *Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies and Laws*, 19 ALB. L.J. SCI. & TECH. 91, 130 (2009) (proposing a model statute that would require all companies to draft privacy policies designed to protect personal information); Kenneth M. Siegel, Comment, *Protecting the Most Valuable Corporate Asset: Electronic Data, Identity Theft, Personal Information, and the Role of Data Security in the Information Age*, 111 PENN ST. L. REV. 779, 810 (2007) (suggesting that companies develop a company-wide strategy to secure electronic information and that consumers, in turn, need to take proactive measures to protect themselves from theft).

32. 18 U.S.C. § 1030 (2005).

33. Pub. L. No. 107-296, § 225, 116 Stat. 2135, 2156.

34. *Id*. § 225(g).

establish procedures to receive complaints about it.[35]

One goal of acts that criminalize and penalize credit card fraud and identity theft, as in the CFAA, CSEA, and ITDA, is to deter would-be criminals. However, political and practical limitations curb the effectiveness of these laws. First, cybercrime is increasingly perpetrated by foreign organized criminals whose governments refuse to extradite these perpetrators.[36] Therefore, these criminals have little reason to fear these laws. Second, in the United States, law enforcement has not been able to keep up with credit card fraud,[37] thus reducing domestic thieves' reasons to fear prosecution under these laws.

Congress also has passed a number of laws to protect consumers from unauthorized credit card charges and losses tied to identity theft. Thus, the Truth in Lending Act[38] ("TILA"), Regulation Z,[39] and the Fair Credit Billing Act[40] ("FCBA") limit consumer liability for unauthorized charges to $50 in most cases.[41] The Identity Theft Enforcement and Restitution Act of 2008 ("ITERA") enables victims of identity theft to seek restitution for money spent restoring their credit and fixing other associated harms.[42] However, none of these laws helps to improve security before the fact.

In fact, while these laws protect victims from some of the "front-end," or direct, costs of fraud, consumers eventually pick up most of the

35. 18 U.S.C. § 1028 (2005).

36. *See* MENN, FATAL SYSTEM ERROR, *supra* note 3.

37. *See* Avivah Litan, *Small Business Account Takeovers Have Regulators, Law Enforcers on the Defense*, GARNTER BLOG (May 12, 2010), http://blogs.gartner.com/avivah-litan/2010/05/12/small-business-account-takeovers-have-regulators-law-enforcers on-the-defense/.

38. The Truth in Lending Act is contained in Title I of the Consumer Credit Protection Act, as amended. 15 U.S.C. § 1601 (2006). This was enacted in 1968 to protect consumers by requiring the disclosure of key terms and costs in lending transactions. *See generally* Matthew Edwards, *Empirical and Behavioral Critiques of Mandatory Disclosure: Socio-Economics and the Quest for Truth in Lending*, 14 Cornell J. L. & Pub. Policy 199 (2005).

39. 12 C.F.R. § 226.1. Regulation Z was promulgated by The Federal Reserve Board to implement TILA pursuant to 15 U.S.C. § 1607. It caps consumer liability for credit card fraud to $50 in most cases. *See generally* Duncan B. Douglas, *An Examination of the Fraud Liability Shift in Consumer Card-based Payment Systems*, 33 ECON. PERSPECTIVES 43-49 (2009).

40. 15 U.S.C. § 1601 (2006).

41. *See, e.g.*, *id.* § 1643 (a)(1)(B) (1980).

42. *See* Pub. L. No. 110-326, 122 Stat. 3560.

tab at the "back-end" in the form of higher prices and other indirect charges. TILA, Regulation Z, FCBA, and ITERA thus may leave consumers with the false impression that someone else will clean up the messes made by cyber thieves, thereby potentially dampening the public will to battle the thieves.

The two laws that come closest to requiring corporations to tackle credit card fraud preemptively are the Fair and Accurate Credit Transactions Act[43] ("FACTA") and the Gramm-Leach-Bliley Act[44] ("GLBA"). FACTA requires merchants to truncate credit card numbers to no more than five digits and refrain from including the expiration dates on receipts.[45] While FACTA is important, it deals only with a tiny part of merchants' vulnerability to hacking. Much more is needed.

The GLBA requires financial institutions "to insure the security and confidentiality of customer records and information"[46] and directs the FTC, along with other government entities, to issue regulations ensuring their protection.[47] The GLBA instructs financial institutions to develop privacy policies and safeguards to protect data, including writing a data security plan detailing the security procedures.[48] The plan must designate at least one employee to manage it; build a comprehensive risk management profile for every department in the institution that handles private information; develop, monitor, and test the data security program; and change the data protection plan as needed to comply with how the data is stored.[49]

While the GLBA seeks to tackle credit card fraud preemptively, it offers few specifics. In fact, the GLBA's entire security guidelines are barely a page long. The law asks that firms have "reasonable measures to protect data"[50] in place. It does not ask that their data be, in fact, secure in any practical sense. The law does not require encryption, passwords, or firewalls – all fairly rudimentary security precautions.

---

43. 15 U.S.C. § 1681 (2003).

44. *Id.* § 6801 (2000).

45. *Id.* § 1681c (g)(1) (2005).

46. *Id.* § 6801(b)(1) (2000).

47. *Id.* § 6801(b)(1)-(3) (2000).

48. 66 Fed. Reg. 8616, 8619-20 (2000). *See also* Fonté, *supra* note 8.

49. *Id.* at 8620-25 (2000). For the mandates, *see* 16 F.R. at 8620 – 8625. *See also* Fonté, *supra* note 8.

50. *See* 16 C.F.R. § 314.4(b) (2002). This subsection is part of what are known as the "Safeguard Rules" – regulations published by the FTC in 2002 to safeguard customer information. *See Companies Comply to Safeguard Rules* (2010), http://www.identitytheft.com/article/companies_safeguard_rules.

Moreover, it seems that firms may not necessarily need to take these precautions to satisfy the law's requirement of "reasonable measures."

Consider the case of *Guin v. Brazos Higher Educ. Serv.*,[51] where the court did not find Brazos, a student loan provider, to have violated the GLBA for allowing an employee to take a laptop home, which the employee subsequently stole along with the unencrypted financial data of 550,000 customers. The court held that, because the loan provider had adequate written security policies, risk assessment reports, and other safeguards, it complied with the GLBA.[52] It did not matter that the firm allowed its employee to regularly download sensitive data on his laptop to work on at home without encrypting the data. Though this might strike many as a glaring red flag, the court held it was not reasonably required by the GLBA.[53]

II. THE MECHANICS OF THE CREDIT CARD INDUSTRY

To understand the structural incentives of the credit card industry, it is important to grasp the mechanics of credit card transactions, their points of vulnerability to fraud, and the way the industry tries to combat these problems. This Part provides that foundation.

A. CREDIT CARD AUTHORIZATION AND SETTLEMENT

Two main series of transactions involve credit cards: authorization and settlement.[54] During the process of authorization, a merchant obtains "permission from the bank that issued the card to accept the card for payment."[55] Settlement is a multi-step process in which the merchant's own bank pays the authorized charge to the merchant and the merchant recovers the charged amount from the authorizing, or issuing, bank.[56] Although authorization and settlement practices vary

51. 2006 WL 288483 (D. Minn. 2006).

52. *Id.* at * 4.

53. *Id.*

54. Ramon P. DeGennaro, *Merchant Acquirers and Payment Card Processors: A Look Inside the Black Box*, 91 FED. RES. BANK ATLANTA ECON. REV. 27, 32 (2006), *available at* http://www.frbatlanta.org/filelegacydocs/erq106_degennaro.pdf.

55. *Id.*

56. *Id.*

somewhat by card brand,[57] we describe herein those used for the two most popular brands: Visa and MasterCard.[58]

1. Authorization

The authorization process starts when a cardholder swipes his or her credit card through a card reader at a merchant, say, Target. Let us assume that the card is a Visa card issued by Bank of America. Target's card reader processes the information from the magnetic stripe, including the card number, expiration date, and verification code.[59] The card reader then electronically transmits the card information, together with the dollar value of the transaction, to a "payment processor," or a company hired by retailers to handle their card transactions.[60] The processor electronically forwards the information to the appropriate Card Association member, as the industry often calls credit card companies, here, Visa.

Visa identifies the "card issuing bank," or "issuer," here, Bank of America, and electronically forwards the information to it for authorization. Bank of America verifies the card information against data it keeps on file and checks whether the cardholder has enough credit to cover the purchase. The card issuer accordingly approves or denies the transaction, and routes its decision back to Target through Visa and the payment processor.[61]

2. Settlement

The settlement process begins when Target electronically submits the day's credit card payments to its payment processor, who forwards them to Target's "acquiring bank," sometimes referred to as the

57. DAVID S. EVANS & RICHARD SCHMALENSEE, PAYING WITH PLASTIC: THE DIGITAL EVOLUTION IN BUYING AND BORROWING 9-12 (2d ed. 2005).

58. American Express and Discover work slightly differently. *Id.* at 12. We focus here on Visa and MasterCard for the sake of simplicity.

59. For a discussion of the security code, *see infra* note 80.

60. Mark Hassinen et al., *Emerging Trends in Information: An Open, PKI-Based Mobile Payment System*, 3995 LECTURE NOTES IN COMPUTER SCI. 86, 92 (2006). There are about 10 U.S. payment processors. *See* First Data Thought Leadership & Rob McMillon, *Where Security Fits in the Payment Processing Chain* (2010), http://www.firstdata.com/downloads/thought-leadership/where_security_fits.pdf.

61. EVANS & SCHMALENSEE, *supra* note 57, at 10.

"acquirer" or "merchant bank." The acquiring bank gives Target a line of credit and agrees to immediately deposit the money due to it from its daily credit card transactions to its bank account (minus various fees). The acquiring bank essentially loans the money to Target until the issuing bank pays the charge. The acquirer sorts and submits Target's credit card transactions to the appropriate Card Association members. So for a transaction with a Bank of America-issued Visa card, the acquirer submits that transaction to Bank of America, which records the transaction in the cardholder's account and pays the acquiring bank (minus fees). The issuing bank later receives payment from the cardholder, usually on a monthly basis. Although these processes seem complex, ever since credit card processing became electronic in 2005, they take mere seconds.[62]

B. CREDIT CARD FRAUD – DISTINCTIONS AND MECHANICS

It is also important to grasp the mechanics of credit card fraud and to distinguish between different types of fraud. One key distinction considers how hackers steal data. The two most common ways are: (1) manually, where the thieves retrieve data during the time that they are infiltrating a computer, and (2) through a concealed automated program, such as a virus or malware installed in the victim's computer system. These programs can "sniff" sensitive data and transmit it back to the hacker until they are discovered, which can take months.[63] The latter is more dangerous than the former because malware lies in wait to copy data as it becomes available, such as when it is being transmitted. Thus, malware can capture data even if the company does not store it. On the other hand, old-fashioned manual hacking is less likely to be able to do so because it is unlikely to infiltrate a system at the precise moment when the data is being transmitted.

Once hackers have the information, they can easily copy it into a

62. Joseph Trigliari, *How Credit Card Processing* Works, *available at* http://www.pivotalpayments.com/ca/industry-news/how-credit-card-processing-works-800343615/.

63. WADE BAKER ET AL., VERIZON RISK TEAM, 2010 DATA BREACH INVESTIGATIONS REPORT 22 (2010), *available at* http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf. Thieves used a sniffer to steal data from over 45 million credit cards as the data was being transmitted from wireless POS systems to TJ Maxx's server. *See* Benjamin Ngugi et al., *PCI Compliance: Overcoming the Challenges*, 3 INT'L J. INFO. SEC. & PRIVACY 54 (2009).

new magnetic stripe to create a counterfeit credit card[64] for use in stores, in what are known as "card-present" transactions. Alternatively, they may use the data to shop over the internet, phone, or mail,[65] in what are known as "card-not-present" transactions. In the latter, the thief needs to convince the store to ship to an address different from the victim's address to avoid alerting the victim, which many thieves have figured out how to do. If the thief steals enough data, he or she may also impersonate the victim's identity and open new accounts in their name.[66]

This raises another important distinction between types of credit card fraud: stealing credit card data from a business's computer network *versus* using a stolen credit card to shop. The former may never result in a loss if the breach is reported and the cards are blocked in time. The latter, however, will result in a loss if the transaction is authorized.

C. THE RULES OF THE GAME: PCI STANDARDS

The credit card industry attempts to protect itself through security standards called the Payment Card Industry Data Security Standard ("PCI DSS"), informally referred to as "PCI standards," "PCI rules," or simply "PCI." The rules came about when, after years of retailer confusion over different company-specific data security standards, the world's five largest credit card companies — Visa, MasterCard, American Express, Discover, and Tokyo-based JCB Co.[67] — formed the "PCI Security Council."[68] In June 2006, they issued the standards.[69]

---

64. Thirty seven percent of all funds stolen through credit cards are stolen with the use of counterfeit cards. *See* Royal Canadian Mounted Police, *supra* note 8.

65. This kind of fraud is sometimes known as "existing" account fraud. Such fraud consists of about 10% of credit card fraud. *See* Royal Canadian Mounted Police, *supra* note 8.

66. C. M. Kahn & W. Roberds, *Credit and Identity Theft*, 55 J. MONETARY ECON. 251, 264 (2008).

67. Fonté, *supra* note 8, at 28.

68. *See* Ngugi et al., *supra* note 63, at 55. *See also* Richardson, *supra* note 5.

69. *See* Press Release, PCI Security Standards Council, Five Leading Payment Brands Unite to Strengthen Global Data Security (Sept. 7, 2006), *available at* https://www.pcisecuritystandards.org/pdfs/09-07-06.pdf. For standards, see PCI Security Standards Council, *The Prioritized Approach to Pursue PCI DSS Compliance*, https://www.pcisecuritystandards.org/documents/Prioritized_Approach_PCI_DSS_1_2.pdf (last visited Aug. 15, 2010). PCI-DSS was started by Visa and MasterCard. Subsequently, the other credit card-issuing companies joined the effort. *See* John Winn & Kevin Govern, *Identity Theft: Risks and Challenges to Business of Data Compromise*, 28 TEMP. J. SCI. TECH. & ENVTL. L. 49, 53-54 (2009).

The standards apply to all companies that accept, store, or transmit credit card data. They require basic measures, such as that firms erect firewalls, encrypt data, keep cardholder data storage to a minimum, and remove security codes from storage after a payment has been authorized.[70]

There is a validation process to make sure that companies are in compliance with the PCI standards. The process is tiered, so that the larger the company as measured by volume of yearly transactions, the more rigorous the validation process. Visa categorizes companies into four tiers, or "Levels." As seen in Table 1, the vast majority of companies (over 6 million) are Level 4 firms, which are small businesses that process fewer than 20,000 online transactions or up to one million store transactions a year.

Table 1

Tiered PCI Compliance Validation Requirements (Visa)[71]

Level	Estimated # of Firms	Number of Visa Transactions Per Year
1	326	over 6 million
2	709	1 million to 6 million
3	3,596	20,000 to 1 million e-commerce transactions
4	over 6 million	less than 20,000 e-commerce transactions and all firms processing up to 1 million transactions a year

The requirement that companies comply with PCI is also embedded in the contracts between the parties involved in authorization and settlement. Instead of negotiating a separate agreement with each issuer, each acquirer simply joins the relevant "card network," an association of banks that issue credit cards,[72] and "agrees to comply with its rules for

70. Other rules that companies must follow include using and regularly updating antivirus software, developing and maintaining the security of the business's systems, and monitoring and analyzing access to secure systems to prevent unnecessary access to information. *See* PCI Security, *The Prioritized Approach*, *supra* note 69.

71. Ngugi et al., *supra* note 63.

72. RONALD J. MANN, CHARGING AHEAD: THE GROWTH AND REGULATION OF

all transactions on that network."[73] The standard network contract between the payment processor and merchant requires the merchant to comply with PCI.[74] Since merchants do not contract directly with the banks or card brands, but only with the payment processor,[75] the issuing and acquiring banks embed their requirements of the merchants in the processor/merchant contract, including PCI compliance.

III. PCI SECURITY RULES ARE BROKEN

A. INEFFECTIVE PCI RULES DESIGNED TO PATCH UP A FLAWED TECHNOLOGY

The PCI security system is broken. The problem is that credit card companies are wedded to a fraud-prone technology: credit cards with magnetic stripes. This technology, which is about forty years old,[76] makes counterfeiting trivially easy.[77] Data on the magnetic stripe is not encrypted. It can be read by the most rudimentary card-reading machines.[78] Thieves can clone it onto another piece of plastic in a matter of seconds, and use it for hundreds of transactions.

In the physical world, credit cards were supposed to be authenticated by cardholders' signatures.[79] However, the reality is that signatures are easy to forge. Few cashiers have the training to identify

---

PAYMENT CARD MARKETS AROUND THE WORLD 20 (2006).

73. *Id*. at 21.

74. *See*, *e.g.*, National Processing Company, *Merchant Processing Agreement: Terms and Conditions*, at 7, *available at* http://images.paysimple.com/files/npc.pdf [hereinafter NPC].

75. The card brands contract with the acquiring banks, who contract with the payment processors, who contract with merchants, and who in turn contract with the service providers. *See* David Navetta, *Who is Minding the Legal Risk Around PCI?*, ISSA JOURNAL, 19 (2009).

76. *See* LEWIS MANDELL, THE CREDIT CARD INDUSTRY: A HISTORY 143 (1990).

77. Dave Whitelegg, *Love it or Hate it, PCI DSS helps cut UK Card Fraud*, *available at* http://blog.itsecurityexpert.co.uk/2010/10/love-it-or-hate-it-pci-dss-helps-cut-uk.html.

78. *See* Jay S. Albanese, *Fraud: The Characteristic Crime of the Twenty-first Century*, *in* COMBATING PIRACY: INTELLECTUAL PROPERTY THEFT AND FRAUD 6 (Jay S. Albanese ed., 2006).

79. *See* GPayments, *An Introduction to Authentication* (2001), *available at* http://www.gpayments.com/pdfs/GPayments_Introduction_to_Authentication_Whitepaper.pdf.

bogus signatures. In addition, signatures are not even possible for online purchases, which were probably never foreseen when the magnetic stripe cards were devised. Yet, instead of investing in safer technologies that depart from the magnetic stripe, the credit card companies built the PCI security system around trying to secure magnetic stripe data.

Consider PCI's key rule prohibiting companies from electronically storing credit card security codes on the back of the cards.[80] The rule assumes that, should hackers steal the magnetic stripe data, they would not be able to use the card because they would not have the security code. In fact, however, the three-digit security code is easy to figure out.[81]

Moreover, even if merchants try not to store security codes, they may do so inadvertently. Most computers and point of sale systems have numerous programs creating logs in different places that store credit card track data.[82] Many merchants lack the sophistication to turn off preferences for logging and storage. Even if those preferences are turned off, certain computer operations are capable of triggering a function that automatically reactivates logging for backup recovery and security purposes.[83] Consequently, what are thought to be impregnable

---

80. *See* DeGennaro, *supra* note 54, at 40. As DeGennaro explains, credit card companies "have long encoded a verification number into the magnetic stripe on the back of the card. Visa calls this code the Card Verification Value (CVV or CVV1); MasterCard's term is the Card Validation Code (CVC or CVC1). This code, read during the swipe, confirms that the card is actually present at the point of sale. The problem is that this approach cannot help for Internet or MOTO transactions because the card is not present and a swipe is impossible." *Id.* PCI Requirement 3 requires merchants to protect cardholder data. *See* PCI Security Standards Council, *The Prioritized Approach*, *supra* note 69; NPC, *supra* note 74, at 7.

81. Three digits can be combined in just 1,000 ways. The difficulty of guessing a password key depends on the number of possible combinations that can be formed with the given password key length. This increases exponentially with increasing password key size: (x^n) where x is the number base (for example 2 for binary and 10 for decimal numbers) and n is the password length. Thus, for a three-decimal digit credit card code security, the number of combinations is 10^3 , which equals 1000. This would take relatively little time to work out with a computer program - hence our assertion that "a three digit code is easy to figure out. *See* M. Whitman & H. Mattord, *Principles of Information Security (2d ed.)(2005).*

82. VeriSign, *Lessons Learned: Top Reasons for PCI Audit Failure and How to Avoid Them*, at 4 (2006), *available at* http://www.verisign.com/static/PCI_REASONS.pdf.

83. *See Automated Event Log Management for PCI DSS Compliance*, at 1 (2009), *available at* http://www.gfi.com/whitepapers/automated-event-log-management-for-

security codes may be easily compromised. The results from one audit revealed that seventy-nine percent of companies do not adequately safeguard sensitive cardholder data, including the security codes.[84]

Another inadequate way in which PCI tries to shore up credit cards is by merely requiring the encryption of cardholder data in "transmission across open, public networks."[85] In so doing, data stored on private networks becomes susceptible to misappropriation by hackers and malicious programs.

B. MONITORING AND ENFORCEMENT OF PCI COMPLIANCE

1. Large Firms: PCI Compliant – But How Safe Are They?

By conducting independent assessments of firms, the card brands have also attempted to enforce a compliance regime for PCI standards. Level 1 firms undergo the most stringent review process,[86] whereas Level 2 and 3 firms enjoy more latitude.[87] Curiously, Level 4 firms escape scrutiny, thus raising serious security concerns.[88] From an enforcement perspective, the card brands may also fine[89] noncompliant and breached businesses and de-list[90] or strip them of the ability to accept credit cards. Just as importantly, an acquirer may refuse to process card payments, resulting in a business's reputational damage for

---

pci-dss.pdf.

84. VeriSign, *supra* note 82, at 4.

85. The Payment Card Industry Data Security Standard outlines twelve requirements designed to improve payment account security, including the encryption of cardholder data across otherwise vulnerable public networks. *See* PCI Security Standards Council, *The Prioritized Approach*, *supra* note 69.

86. *See* Visa, Inc., *Data Security Bulletin: Visa PCI DSS Compliance Validation Framework* 2-3 (Nov. 18, 2008), *available at* http://usa.visa.com/download/merchants/cisp-bulletin-visa-pci-dss-framework-111808.pdf.

87. *See* Ponemon Institute Report, *PCI DSS Compliance Survey* (Sept. 24, 2009), *available at* http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/PCI%20DSS%20Survey%20Key%20Findings%20FINAL4.pdf.

88. *See* Joan Herbig, *Level 4: The small merchant PCI challenge* (Apr. 27, 2009), *available at* http://www.greensheet.com/gs_online.php?story_id=1319.

89. *See infra* Part IV.

90. *See* ControlScan et al., *What Small Merchants Know (and Don't Know) about PCI Compliance: A Research Report* (2009), *available at* http://www.nrf.com/modules.php?name=Documents&op=showlivedoc&sp_id=3511; *see also* DeGennaro, *supra* note 54.

failure to service clients.[91] PCI's enforcement program has proven resoundingly effective, as evidenced by the high compliance rates for Level 1 and 2 firms (96% and 95%, respectively).[92]

Despite the resources available to the card brands, it remains unclear to what degree PCI compliance ensures reliable security. For purposes of illustration, twenty-one percent of businesses validated as PCI compliant during their most recent PCI assessments fell prey to credit card fraud.[93] With one exception, the businesses from this sample were grouped in the Level 1 category[94] (and, by definition, were the subjects of comprehensive PCI assessments). For example, Heartland, a large payment processor, was PCI compliant, but was the target of a successful hacking attack.[95] More disturbing, Hannaford Brothers, a large, reputable supermarket chain, was in the process of being recertified as PCI compliant even as malware infected servers at each of its approximately 300 stores, transmitting millions of credit card numbers to thieves over a period of months.[96]

2. Small Firms: The Weakest Link

PCI enforcement of Level 4 firms lacks definable parameters. From a logistical standpoint, the PCI Council cannot monitor all Level 4 firms – that is, a total of approximately six million businesses. The Council, therefore, requires that Level 4 firms complete individual self-assessment forms,[97] the contents of which are seldom meaningfully challenged.

As a general proposition, though, the vast majority of Level 4

---

91. *See* Ellen Libenson, *Dollars and Sense: Calculating PCI Noncompliance Costs*, E-COMMERCE TIMES, Dec. 12, 2007, *available at* http://www.technewsworld.com/story/60712.html.

92. Visa, Inc., *U.S. PCI DSS Compliance Status* (June 30, 2010), http://usa.visa.com/download/merchants/cisp_pcidss_compliancestats.pdf.

93. *See* BAKER ET AL., *supra* note 63, at 53.

94. *Id.*

95. Warwick Ashford, *Heartland Data Breach Proves PCI Compliance Is Not Enough*, COMPUTERWEEKLY.COM, Jan. 26, 2009, http://www.computerweekly.com/Articles/2009/01/28/234421/Heartland-data-breach-proves-PCI-compliance-is-not-enough.htm.

96. Andrew Conry-Murray, *Hundreds of Servers Compromised in Hannaford Breach*, INFORMATIONWEEK'S SEC. WEBLOG (Mar. 28, 2008, 3:44 PM), http://www.informationweek.com/blog/main/archives/2008/03/hundreds_of_ser.html.

97. Visa, *Data Security Bulletin*, *supra* note 86.

companies are noncompliant.[98] Indeed, an alarming number of Level 4 merchants do not adhere to the most elementary of PCI rules, such as the rule on encryption.[99] Despite this, Level 4 business' compliance levels continue to decrease.[100] The failure to remedy this situation is important because Level 4 merchants collectively account for 99 percent of all credit card transactions in the United States.[101] These firms unleash the highest number of data breaches[102] and "are increasingly a larger percentage of compromise incidents."[103] One survey found them responsible for 85 percent of all credit card breaches.[104]

The problem is that credit card companies give small merchants no incentive to be compliant. Since they rely solely on trust and do not verify the merchants' self assessment forms, credit card companies are unlikely to fine or delist these merchants for noncompliance until after a breach is discovered. At the same time, the credit card companies and banks fail to reward Level 4 firms for compliance or subsidize their expenses, even though research shows that most of these firms cannot afford to comply with PCI.[105] Cost stands as "the main obstacle," as one study concluded.[106] Compliance can cost around $81,000 for a small

98. *See, e.g.*, Mike Masin, The *Cost of PCI Non-Compliance for Small Businesses (Part 3 of 3)*, THE VIEW FROM UNDER THE HAT (Jan. 25, 2010), http://m2.atstuff.com/the-cost-of-pci-non-compliance-for-small-businesses-part-3-of-3/. *See also PCI Compliance Fines For Small Business Breaches*, BRAINTREE (Oct. 18, 2007), http://www.braintreepaymentsolutions.com/blog/pci-related-fines-for-breaches-at-small-businesses (finding that, since 2005, over 80 % of card breaches have occurred at small merchants).

99. Jaikumar Vijayan, *Update: New Retail Data Breach May Have Affected Millions of Hannaford Shoppers*, COMPUTERWORLD (Mar. 17, 2008, 12:00 PM), http://www.computerworld.com/s/article/9068999/Update_New_retail_data_breach_may_have_affected_millions_of_Hannaford_shoppers.

100. PONEMON INST, *supra* note 10.

101. Masin, *The Cost of PCI Non-Compliance*, *supra* note 98.

102. *See, e.g.*, *id. See also* BRAINTREE, *supra* note 98.

103. Mike Masin, *Fraud Prevention for Small Business Owners*, THE VIEW FROM UNDER THE HAT (Feb. 12, 2010), http://m2.atstuff.com/fraud-prevention-for-small-business-owners/.

104. Kelly Jackson Higgins, *National Retail Federation Poll: Small Retailers Struggling To Understand PCI*, DARKREADING.COM (Aug. 11, 2009, 3:46 PM), http://www.darkreading.com/story/showArticle.jhtml?articleID=219200246.

105. Penelope N. Lazarou, Note and Comment, *Small Businesses and Identity Theft: Reallocating the Risk of Loss*, 10 N.C. BANKING INST. 305, 315 (2006); *See also* Masin, *The Cost of PCI Non-Compliance*, *supra* note 98.

106. PONEMAN INST., *supra* note 10, at 1.

business, though that number will vary depending on its precise size and complexity, in addition to outlays to keep pace with security developments.[107] For "'mom and pop' dry cleaners, pizza parlors, and convenience stores," that is too expensive.[108] Thus, many small businesses decide to gamble, viewing the risk of hacking as "a simple numbers game."[109]

3. Incoherence in Action: Forcing Merchants to Jeopardize Their Security

Ironically, the acquiring banks, which require merchants to be PCI compliant,[110] also essentially require them to jeopardize their security. The banks embed in the merchant-processor contract a provision that the merchants must store credit card data in their computers for one to two years.[111]

Storing sensitive data, however, turns merchants into magnets for hackers – especially since PCI rules to protect stored data are so inadequate. Merchants are told that they must provide the acquiring bank with this stored data in the event of a "retrieval request" by the Card Issuer, which occurs when a cardholder disputes a charge and wants it reversed, when there is a point of sale error, or when there is a fraud inquiry.[112] The banks and card brands, however, already keep electronic copies of these same records.[113] Therefore, it is hard to understand why they force businesses to store this sensitive data – other than that it is convenient for them. It is easier to have the merchant search for and produce a document rather than to do it themselves.

Ironically, however, it is not necessary to require merchants to store

---

107. *See* Pui-Wing Tam & Robin Sidel, *Security-Software Industry's Miniboom*, WALL ST. J., Oct. 2, 2007, at B3, *available at* http://online.wsj.com/article/SB119128527341745878.html.

108. ControlScan et al., *What Small Merchants Know*, *supra* note 90, at 9.

109. Bob Sullivan, *Instant Credit Means Instant Identity Theft*, MSNBC.COM (May 25, 2005), http://www.msnbc.msn.com/id/6762127/.

110. *See* discussion *supra* note 75 and accompanying text.

111. *See* NPC, *supra* note 74, at 16.

112. *See id*. at 11. *See also* Chase Bank, *Handling Retrieval Requests*, CHASE.COM, https://www.chase.com/cm/crb/sbfs/page/request.html (last visited Nov. 18, 2010).

113. The credit card companies and issuing banks keep copies of the data they transmit during the authorization and settlement processes. *See* DeGennaro, *supra* note 54.

credit card data for the sake of satisfying retrieval requests related to disputes, errors, or investigations. While it may have been necessary historically, when manual credit card punch machines were used[114] and a merchant's only record of a transaction was the paper duplicate,[115] today, the information is electronic, and can be used in that form to settle the said retrieval requests.

4. Tokenization Could Solve the Problem of Unsafe Data Storage for Retrieval Requests: But is it Used?

Moreover, merchants could satisfy the same retrieval requests without storing any credit card data. With tokenization, the substitution of the credit card number with a string of other numbers called a token,[116] merchants store the token, not the credit card number or other data on the card's magnetic stripe. Rather, the payment processor or bank keeps the credit card number and associated data in a secure server or "vault," and is able to map tokens to their corresponding credit card numbers. The logic of tokenization is based on the premise that it is easier to secure one central vault than multiple company networks.[117] In the event of a retrieval request, the party that controls the vault would get the cardholder credit card number and transaction details from the cardholder or issuer, pass the matching token to the merchant and ask for the electronic receipt. Production of the matching receipt by the merchant would show the authenticity of the transaction.[118]

In July 2010, Visa publicly agreed, in a nod to the National Retail

---

114. Sankarson Banerjee, *Credit Card Security on the Net: Where is it Today*?, 12 J. FIN. TRANSFORMATION 21, 21-23 (2004).

115. Douglas Akers et al., *Overview of Recent Developments*, 17 FDIC BANKING REV. 3, 23 (2005).

116. Avivah Litan & John Pescatore, *Using Tokenization to Reduce PCI Compliance Requirements*, GARTNER.COM (2009), http://www.gartner.com/DisplayDocument?doc_cd=169939&ref=g_fromdoc; Gary Palgon, *Best Practices In Data Protection*, RETAIL SOLUTIONS ONLINE (Apr. 21, 2010), http://www.retailsolutionsonline.com/article.mvc/Best-Practices-In-Data-Protection-0002.

117. *See* First Data & McMillon, *supra* note 60, at 3, 12-13.

118. *See* HEATHER MARK, SHIFT4 SECURE PAYMENT PROCESSING, STORING CREDIT CARD DATA: A LOOK AT THE BUSINESS NEEDS, REGULATIONS AND SOLUTIONS REGARDING THE ISSUE 7 (2006), http://www.shift4.com/pdf/s4-wp0801_storing-credit-card-data.pdf; First Data & McMillon, *supra* note 60, at 12.

Federation's long-standing complaints,[119] that merchants should not be obligated to store credit card numbers for retrieval requests[120] and indicated that acquiring banks should allow merchants to use tokenization.[121] While this is a first step, it is hard not to wonder if it is an empty magnanimous gesture. PCI is the organ through which security changes are implemented in the industry. There is no movement to reflect these changes there. Moreover, it does not seem there will be any changes made any time soon: PCI is controlled by five credit card companies, none of which has joined Visa's statement.

The silence and lack of movement surrounding storage and tokenization are telling, since tokenization requires a top-to-bottom approach to work effectively. Those at the top must keep the credit card data in a vault, while those at the bottom must keep the tokens.[122] As one expert has stated, tokenization would "require the development and implementation of a new payment processing protocol. All card processors would need to certify with the card brands that they can process the new payment systems, and all point-of-sale (POS) systems would need to be both modified and certified for the new protocol."[123]

5. PCI Does Not Aggressively Push for New Security Technologies that Change the Status Quo

The card companies' passivity on tokenization is symptomatic of

---

119. *See, e.g.*, Letter from David Hogan, Chief Information Officer, National Retail Federation, to Bob Russo, PCI Security Standards Council, LLC (Oct. 2, 2007), *available at* http://www.nrf.com/modules.php?name=News&op=viewlive&sp_id=380; *see also* Marcia Savage, *Visa: Banks Shouldn't Force Merchants To Store Full Card Data*, SEARCHFINANCIALSECURITY.COM (July 15, 2010), http://searchfinancialsecurity.techtarget.com/news/article/0,289142,sid185_gci1516765,00.html.

120. Visa Inc., *Visa Best Practices for Primary Account Number Storage and Truncation* (July 14, 2010), http://usa.visa.com/download/merchants/PAN_truncation_best_practices.pdf.

121. *See* Savage, *supra* note 119, at 1 ("Acquirers and issuers must allow merchants to present 'a truncated, disguised or masked card number on a transaction receipt' for dispute resolution . . . [since] the unnecessary storage of full Primary Account Numbers (PANs) by merchants has led to data compromise, theft and unintentional disclosure . . . .").

122. Avivah Litan, *Proposed PCI Changes Would Improve Merchant's Data Security*, GARTNER.COM (Oct. 10, 2007), http://www.gartner.com/DisplayDocument?doc_cd=152561.

123. *Id*.

their overall approach to security. Although the technology sector is highly innovative,[124] the card brands do not push hard for the industry to adopt new solutions that would alter the status quo.

Take "chip and PIN" technology.[125] It replaces the magnetic stripe on the credit card with a smartcard that has an embedded microchip. The cardholder swipes his or her smart card and enters his or her personal identification number ("PIN"). The use of a PIN makes hacking harder because some of the information needed to conclude a sale rests in the cardholder's memory. Not all of it is on the card, as with the traditional credit card. Furthermore, the data on the chip-card remains useless until it is decrypted using the PIN.

Yet, chip and PIN technology has not made inroads either with PCI or with card companies,[126] despite its proven track record in lowering fraud. France, for instance, introduced a chip-based PIN system in 1993 and saw counterfeiting fall by 78 percent and fraud losses by 50 percent in the first year.[127] By 1996, counterfeiting charges effectively had been eliminated. By 1998, banks were saving about 0.1 percent of sales volume on fraud.[128] In the United Kingdom ("UK"), the "success of chipand PIN has meant that over the past four years losses on transactions on the UK high street have reduced by 67% from £218.8m in 2004 to £72.1m in 2009."[129]

PCS has also overlooked many other robust technologies. Take end-to-end encryption ("E3"), in which cardholder data is encrypted from the point of sale until it is received by the payment processor. E3 can reduce vulnerability to malware, particularly when combined with tokenization.[130] New data-mining technologies also can help protect

---

124. *See e.g.*, *Payment Security Solutions*, CYBERSOURCE.COM, http://www.cybersource.com/products_and_services/payment_security/ (last visited Nov. 18, 2010).

125. CHIP AND PIN, http://www.chipandpin.co.uk (last visited Nov. 18, 2010).

126. *See* Claes Bell, *Are Chip and PIN Credit Cards Coming?*, FOX BUS. (Feb. 17, 2010), http://www.foxbusiness.com/personal-finance/2010/02/17/chip-pin-credit-cards-coming/.

127. Sushila Nair, *Why the Adoption of Chip and PIN Technology is Inevitable*, SECURE THINKING (Dec. 8, 2009), http://www.btsecurethinking.com/2009/12/why-the-adoption-of-chip-and-pin-technology-is-inevitable/.

128. *Id.*

129. UK Payments Admin., *Card Fraud Facts and Figures*, http://www.ukpayments.org.uk/resources_publications/key_facts_and_figures/card_fraud_facts_and_figures/ (last visited Nov. 18, 2010).

130. *See* First Data & McMillon, *supra* note 60. *See also*, Thomas Claburn, *Credit*

merchants from online fraud by identifying and preventing criminals trying to use stolen credit cards.[131]

6. Leadership is Needed to Coordinate the Implementation of New Technologies System-wide: Where is it?

Implementing new technologies requires leadership from the credit card companies for a number of reasons. First, some technologies, such as Chip and PIN, require broad implementation to work. It would be pointless for a merchant to invest in PIN technology today since U.S. payment systems do not support it. Broad implementation is best coordinated from the top.

Second, system-wide coordination is often needed to ensure that merchants who use the new technologies of a bank or payment processor are not locked into a relationship with them. For example, imagine that a payment processor offers to tokenize a merchant's data *gratis*. The merchant, enticed by the free offer, signs up. A year later, however, the processor raises rates substantially. Unless the industry has a system-wide process for tokenization, the merchant would be stuck with the initial processor. A new processor could not map or decipher the tokens for lack of the original mapping file. The initial mapping tables belong to the original processor. A uniform process might ensure that merchants "own" their data, but the payment processor or bank would hold it in trust for them so that when they move to a new institution, the original institutions transfers it for them.

IV. CAUSES OF THE PROBLEM: WHY THE CREDIT CARD INDUSTRY MAY NOT BE INTERESTED IN SEEING DATA SECURITY REFORM

The General Manager of the PCI Security Council recently conceded that the Council is interested in fighting credit card fraud only

---

Card Processors Getting Encryption Religion, INFORMATIONWEEK (Nov. 21, 2009), http://www.informationweek.com/news/security/encryption/showArticle.jhtml?articleID=221900322.

131. *See Show Me How It Works*, THREATMETRIX, http://threatmetrix.com/our-solutions/show-me-how-it-works/ (last visited Nov. 18, 2010). PCI, however, focuses only on protecting credit card data *before* it is stolen. It glosses over protecting merchants against the use of credit card data that has already been stolen.

if it can do so "within the existing system."[132] Why this limitation? This section of the article explores the financial incentives and the historical background that lie at the root of this attitude.

A. FOLLOW THE MONEY: THE CREDIT CARD INDUSTRY'S LACK OF INCENTIVES TO INITIATE FAR-RANGING ANTI-FRAUD REFORMS

1. Credit Card Companies' Incentives

Overall, credit card companies do not have strong incentives to get serious about fraud on an industry-wide, systemic basis. They get paid every time their credit card is used, even in fraudulent transactions. Their revenue mostly comes from "assessment fees," a percentage of the price of every purchase made using their card brand – 0.0925 percent for Visa and 0.0950 percent for MasterCard and Discover.[133] The fee is not returned in the event of fraud. They can also collect fines when companies are breached.[134] This insulates the companies from the immediate financial effects of credit card fraud.

Credit card companies may also have good reason to avoid trying new technologies that could jeopardize their revenue. If "chip and PIN" technology were used on credit cards, for example, card data might be transmitted across existing networks used for PIN debit cards rather than across credit card networks. If so, companies that operate PIN networks, like NYCE and Star,[135] would profit, while credit card companies might not profit.

This is not to say that credit card companies do not care about fraud in the industry. They did, after all, establish PCI. However, it is likely that their biggest concern regarding fraud in the industry is keeping it

---

132. Anton Chuvakin, *RSA 2010 Exclusive PCI Security Standards Council Interview*, SECURITY WARRIOR BLOG (Mar. 12, 2010), http://chuvakin.blogspot.com/2010/03/rsa-2010-exclusive-pci-security.html (last visited Nov. 18, 2010).

133. *See* Electronic Exchange Systems, *Merchant Credit Card Processing Agreement* (2009), *available at* http://www.oneclickdining.com/images/pdf/MOTO_setup.pdf.

134. *See* Higgins, *supra* note 104. Card Association members can fine acquiring banks between $5,000 to $100,000 per month for PCI compliance violations and merchants and other players between $5,000 to $25,000 a month. *Id.*

135. Barbara Pacheco & Richard Sullivan, *Interchange Fees in Credit and Debit Card Markets: What Role for Public Authorities?*, FED. RESERVE BANK KANSAS CITY ECON. REV. 92 (2006), *available at* http://www.kansascityfed.org/publicat/econrev/PDF/1q06pach.pdf.

from reaching such high levels that it would scare significant numbers of customers from using cards because their profits depend on transaction volume. It would probably take an enormous scandal before concerns of fraud caused consumers to stop using credit cards, for several reasons.

First, credit cards are highly convenient.[136] Second, perceptions of fraud levels, rather than real fraud levels, are what truly matter with respect to frightening customers. In this regard, credit card companies benefit from the fact that accurate measures of credit card fraud are notoriously difficult to find.[137] It is suspected that credit card fraud is vastly underreported.[138] Real figures are shrouded in secrecy. No federal repository for data breach information exists.[139] State breach notification laws are so riddled with loopholes as to make them virtually useless.[140] PCI rules prohibit its investigators and assessors from disclosing any information acquired in the line of service about noncompliance or breaches.[141] Menn suggests that the card companies and banks profit so much from the underreporting of fraud that they "didn't just keep quiet" about it, but also "actively worked to distort the public discourse," sponsoring, in one case, a seemingly objective report that downplayed the severity of the problem.[142]

In fact, lulling consumers into a sense of security about credit card fraud has been an industry priority. One of the industry's broadest initiatives was implementing a "zero-liability policy,"[143] under which

136. Scott Schuh et al., *Who Gains and Who Loses from Credit Card Payments?: Theory and Calibrations*, (Fed. Reserve Bank of Boston, Paper No. 10-3, 2010), *available at* http://www.bos.frb.org/economic/ppdp/2010/ppdp1003.pdf.

137. Ben Ngugi et al., *Evaluating the Quality and Usefulness of Information from Current Data Breach Notification Systems* (2010) (unpublished manuscript) (on file with International Journal of Information Security and Privacy).

138. *Identity Theft Laws – How the Legal System Can Protect You*, EMAILSCAMMERS.COM, http://www.emailscammers.com/identity-theft-laws-how-the-legal-system-can-protect-you/ (last visited Nov. 18, 2010).

139. *See* Ngugi et al., *supra* note 137.

140. *Id.*

141. *See* PCI Securities Standards Council, *Qualified Security Assessor (QSA) Agreement*, app. A, *available at* https://www.pcisecuritystandards.org/pdfs/pci_qualified_security_assessor_qsa_agreement.pdf (stipulating in clause A.6.1 that the QSA agreement contract requires total confidentiality).

142. *See* MENN, FATAL SYSTEM ERROR, *supra* note 3, at 116.

143. *See, e.g.*, *MasterCard Zero Liability*, MASTERCARD.COM, *available at* http://www.mastercard.com/us/personal/en/cardholderservices/zeroliability.html (last visited Nov. 18, 2010); *Visa Security Program: Zero Liability*, VISA.COM, *available at*

victimized consumers generally pay nothing for unauthorized charges, less even than the $50 they would otherwise pay under TILA[144] and Regulation Z.[145] As one expert noted:

> It seems that all of the security improvements that the 'credit card industry' (meaning the issuing banks and card brands) puts out there are aimed at the consumer. . . . And that makes sense, because the 'credit card industry' wants consumers to trust their product and use them as their preferred payment instrument.[146]

Unfortunately, manipulating public perception of danger is much easier than tackling the reality of criminals' ability to hold the credit card system hostage. As long as those perceptions continue and card companies do not feel the financial repercussions of fraud, it would be unreasonable to expect drastic change in their attitude towards security on an industry-wide basis.

2. Issuing Banks' Incentives

Most people think that the issuing bank bears the brunt of credit card fraud losses,[147] for it is the issuing bank that consumers call when they see unauthorized charges on their bills, and that seems to cover those costs.[148] In reality, however, issuers shift much of the cost of credit card fraud to the retailer who sold the goods to the thief. First, by contract, issuing banks only absorb credit card losses when the thief makes the purchase in person, known as "card present" transactions.[149] The retailer, however, takes the hit when the thief makes the purchase

---

http://usa.visa.com/personal/security/visa_security_program/zero_liability.html.

144. 15 U.S.C. § 1643 (a)(1)(B) (2009).

145. 12 C.F.R. § 226.12(b)(1) (2008); *see also* Duncan B. Douglass, *An Examination of the Fraud Liability Shift in Consumer Card-based Payment Systems*, 33 ECON. PERSP. 43 (2009).

146. Robert McMillon, *Helping the Merchant*, SPEAKING OF SECURITY: THE OFFICIAL RSA BLOG AND PODCAST (July 13, 2010), http://blogs.rsa.com/mcmillon/helping-the-merchant/ (last visited Nov. 18, 2010).

147. *See* MENN, FATAL SYSTEM ERROR, *supra* note 3, at 116.

148. Douglass, *supra* note 145, at 47.

149. *See, e.g.*, Visa, Inc., *Visa International Operating Regulations* 881-88, 893-901 (2010), *available at* http://usa.visa.com/download/merchants/visa-international-operating-regulations-main.pdf; *see also* MasterCard Worldwide, *Chargeback Guide* (2010), *available at* http://www.mastercard.com/us/merchant/pdf/TB_CB_Manual.pdf. *See generally*, Douglass, *supra* note 145.

over the phone, internet, or by mail, known as "card-not-present" transactions.[150] Under this arrangement, merchants absorb about twice as much loss as issuers, since online fraud is thought to cost twice as much as in-person fraud.[151]

Nevertheless, the issuing bank can charge back to the retailer all fraudulent "card-present" sales in which the retailer failed to obey a contractual requirement. Therefore, if the signature on the receipt does not match the signature on the credit card, the issuer can charge the retailer for the fraud on the grounds that he or she failed to verify the signature, as required by contract.[152] Banks charge the merchants $25 to $35 for every such "charge-back."[153] Observers suggest that the number of charge-backs is growing as issuing banks selectively choose[154] retail transactions in a concerted industry effort to shift at least some of the liability to retailers.[155]

The second manner in which issuing banks can shift some of the costs of fraud to merchants is through interchange fees. The less competitive a market is, the more a business can increase prices without losing market share.[156] The market for interchange fees is rather uncompetitive.[157] The card brands set the interchange fees and the

150. MasterCard, *Chargeback Guide*, *supra* note 147, at 6-7. The merchant absorbs the loss unless he or she "1) performed an address verification at the time the transaction was authorized (that is, verified that the person conducting the transaction could validate the billing address associated with the payment card being used); 2) delivered the purchased merchandise to an address that matches the address validated through the address verification; and 3) obtained proof that the purchased goods were delivered to the verified address." Douglass, *supra* note 145, at 45-6. *See also* NPC, *supra* note 74, at 12.

151. KEN PATERSON, MERCATOR ADVISORY GRP., CREDIT CARD ISSUE FRAUD MANAGEMENT (2008), http://www.sas.com/news/analysts/mercator_fraud_1208.pdf.

152. *See, e.g.*, *Visa International Operating Regulations*, *supra* note 149, at 464; *see also Fraud Control Basics: Card-Present*, VISA.COM, *available at* http://usa.visa.com/merchants/risk_management/card_present.html.

153. Robert Berner & Adrienne Carter, *The Truth About Credit-Card Fraud*, BUSINESSWEEK (June 21, 2005), www.businessweek.com/technology/content/jun2005/tc20050621_3238_tc024.htm.

154. *Id*.

155. *Id*.

156. *See generally*, Jean-Charles Rochet & Jean Tirole, *Cooperation Among Competitors: Some Economics of Payment Card Associations*, 33 RAND J. ECON. 549 (2002).

157. *See* Adam J. Levitin, *Payment Wars: The Merchant-Bank Struggle for Control of Payment Systems*, 12 STAN. J.L. BUS. & FIN. 425, 426-31 (2007).

issuing banks agree to impose them.[158] There is no competition among the banks to lure merchants to accept a particular credit card brand by lowering the fees. In fact, with Visa and MasterCard controlling around 80 percent of volume of credit card transactions,[159] the card brands wield such a large degree of market power that retailers have little choice but to pay the fee.[160]

The only competition regarding interchange fees comes from the credit card companies themselves. They compete to have issuing banks issue their brand of credit card by offering to set higher interchange fees than their rivals.[161] This competition increases prices for merchants.[162] Indeed, American interchange fees, which are now between one to three percent of the purchase price of each transaction,[163] have been rising steadily since 2000[164] despite bitter protests from retailers.[165] The

158. Andrew Martin, *The Card Game: How Visa, Using Card Fees, Dominates a Market*, N.Y. TIMES, Jan. 4, 2010, at A1, *available at* http://www.nytimes.com/2010/01/05/your-money/credit-and-debit-cards/05visa.html?_r=1.

159. *See* Maria Aspan, *Visa, MasterCard Growth May Outweigh Regulations*, REUTERS, May 20, 2010, *available at* http://www.reuters.com/article/idUSN2022077920100520. *See also* Nilson Report, *supra* note 15 (explaining Visa controlled 64.79% of the 2009 global market share in terms of volume of purchase transactions, MasterCard controlled 26.5%, and American Express controlled 4.57%).

160. *See* Adam Levitin, *Credit Card Fair Fee Act*, CREDIT SLIPS, (Mar. 30, 2008, 7:51 PM), http://www.creditslips.org/creditslips/2008/03/credit-card-fai.html. The barriers to enter the credit card industry are high. Even if a new rival offered a lower interchange rate, as long as customers preferred existing brands, the company could not succeed. Indeed, no business has entered the market since Discover did in 1985. It would be difficult to get customers because issuing banks, who pocket the interchange fees, would want to go with the card brand that offered them the highest fee. Proprietary cards, such as an Amazon.com card, are accepted only at a single retailer and do not realistically substitute for general purpose cards such as a Visa card. *Id*.

161. *See* Rochet & Tirole, *supra* note 156.

162. *See* Martin, *supra* note 158. Vigorous competition by the card brands on interchange fees has the unusual effect of raising prices for merchants, not lowering them. Card companies vie for issuing banks' business by offering higher interchange fees and make their cards more appealing by offering higher interchange fees. The card companies do not compete for merchants' business. As a result, there is currently upward pressure on interchange fees. *See id.*

163. *Id*.

164. *Id*.; *see also* Getahn Ward, *Merchants Pay More to Accept Credit Cards*, THE TENNESSEAN, Apr. 8, 2010, *available at* http://www.tennessean.com/article/20070408/BUSINESS01/704080362/Merchants-pay-more-to-accept-credit-cards ("Most interchange costs come as a flat fee of 10 to 25 cents per transaction, plus a percentage of the sale, about 2 % on average. Thus, a $100 purchase would include $2

interchange fees charged are the highest in the world,[166] yet, as one court found in 2001, "both Visa and MasterCard have raised prices and restricted output without losing merchant customers."[167] American courts have not yet held that interchange fees violate antitrust laws.[168]

Issuing banks can also slip the bill to consumers through higher credit card and banking costs. Although the 2009 Credit Card Accountability, Responsibility, and Disclosure Act of 2009 ("Credit Card Act")[169] plugged a number of revenue streams that the banks enjoyed from credit cards, such as high over-draft fees,[170] plenty of

---

or slightly more in fees, which the credit card company shares with the bank that issued its card and the bank that processes the purchase for the merchant.").

165. *See* MANN, CHARGING AHEAD, *supra* note 72.

166. *See* Levitin, *Payment Wars*, *supra* note 157, at 462.

167. United States v. Visa U.S.A. Inc., 163 F. Supp. 2d 322, 342 (S.D.N.Y. 2001).

168. *See* Steven Semeraro, *Credit Card Interchange Fees: Three Decades of Antitrust Uncertainty*, 14 GEO. MASON L. REV. 941, 996 (2007). Not all uncompetitive situations, however, meet the law's definition. The Sherman Act does not, for example, prevent monopoly status that is earned through good business decisions. *See* United States v. Aluminum Corp. of America, 148 F.2d 416, 429-30 (S.D.N.Y. 1945). Furthermore, some commentators feel that some of the past interchange fee antitrust cases were wrongly decided and, therefore, are not truly dispositive. *See, e.g.*, Levitin, *Credit Card Fair Fee Act*, *supra* note 160. Indeed, antitrust litigation concerning interchange fees remains very much alive. One case pending in the Eastern District of New York consolidates forty actions against Visa and MasterCard. *See In re* Payment Card Interchange Fee & Merch. Disc. Antitrust Litig., 562 F.Supp. 2d 392 (E.D.N.Y. 2008). In addition, Europe has found interchange fees to violate its antitrust laws. The European Commission's antitrust authority ruled in 2008 that MasterCard's interchange fees were illegal. Press Release, European Commission for Competition Policy, Commission Prohibits MasterCard's Intra-EEA Multilateral Interchange Fees (Dec. 19, 2007), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/07/832&format=HTML&aged=0&language=EN&guiLanguage=en. In 2009, the European Commission's antitrust authority charged that Visa's interchange fees were also illegal. *See EC Hits Visa Europe with Interchange Antitrust Charge*, FINEXTRA.COM (Apr. 6, 2009, 4:18 PM), http://www.finextra.com/news/fullstory.aspx?newsitemid=19881; *see also* Press Release, Visa, Inc., Settlement on Visa Debit Interchange Fees Aids SEPA (Apr. 26, 2010), *available at* http://www.visaeurope.com/en/newsroom/news/articles/2010/visa_interchange_fees_aid_sepa.aspx; Matthew Dalton & Pepp Kiviniemi, *EU Charges Visa Europe Over Fees*, WALL ST. J., Apr. 7, 2009, at C2, *available at* http://online.wsj.com/article/SB123902543327292827.html.

169. Pub. L. No. 111-24, 123 Stat. 1734 (2009).

170. 12 C.F.R. § 205.17 (2009).

loopholes remain.[171] All this blunts the urgency that banks might otherwise feel to initiate broad, system-wide anti-fraud strategies that cover merchants and other stakeholders.

Issuing banks may also feel that they are doing enough to bring fraud down to acceptable levels. Most use neural networks to track individual cardholder purchases and spending habits. The network's ability to alert the bank to transactions that do not fit those habits[172] has helped mitigate certain kinds of fraud, and may give the banks a sense that they are doing enough. However, the technology is not failsafe.[173] Moreover, the banks' adeptness at diverting their losses likely colors their evaluation of what is enough to decrease fraud.

3. Acquiring Banks' Incentives

Some people think that if the merchant is hacked, the acquiring bank pays for the damages, including fines.[174] Visa publicly reports that it fines acquiring banks hundreds of millions of dollars a year for their merchants who are breached while not compliant with PCI.[175] However, card brands fine the acquiring banks when the merchant has been hacked because the credit card company's contract is with the acquiring bank, not the merchant.[176]

However, it is less well known that acquiring banks are contractually entitled to indemnification by merchants for any losses they incur as a result of the breach, including fines.[177] Acquiring banks deduct the amount of the fine and any other losses it incurred from the merchant's bank account.

Acquiring banks also can offset fraud losses indirectly through the

---

171. Jaclyn Rodriguez, *The Credit Card Act of 2009: An Effective But Incomplete Solution Evidencing the Need for a Federal Regulator*, 14 N.C. BANKING INST. 309, 328 (2010).

172. Craig Bicknell, *EFalcon Preys on Credit Card Fraud*, WIRED (May 13, 1999), http://www.wired.com/techbiz/media/news/1999/05/19662.

173. *See* Jay MacDonald, *Fraud, Identity Theft, Grow at ATMs*, CARDSWITCHTECHNOLOGY.COM (Jul. 17, 2008), http://www.cardswitchtechnology.com/Documents/News3.pdf.

174. *See, e.g.*, Sasha Romanosky & Alessandro Acquisti, *Symposium: Security Breach Notification Six Years Later: Privacy Costs and Personal Data Protection: Economic and Legal Perspectives*, 24 BERKELEY TECH. L.J. 1061, 1077 n.80 (2009).

175. *Id*. at 1077 n.81-84.

176. *See* Navetta, *supra* note 75, and related discussion.

177. *See* NPC, *supra* note 74, at 6.

discount fees they charge retailers, which is now 0.07 percent per transaction.[178] All this would weaken acquiring banks' incentives to effect broad-based changes.

B. FOLLOW THE HISTORY: WHY THE ATTITUDE TOWARDS DATA SECURITY IS SO INSULAR

The historical roots of the two largest card brands, Visa and MasterCard, provide another way to understand why the card brands and banks seem so self-interested in their approach to security. From the 1960s, when they came into being, and until recently, the main card brands were structured as not-for-profit membership associations owned by issuing and acquiring banks.[179] In contrast to regular stock corporations, in which shareholders tend not to have direct outside business relationships with the firm, a membership association's members do business with and are involved in running the association. Each member received a certain number of votes to influence how the association was run.[180] The higher a member's yearly volume of transactions, the more votes it held.[181] Members selected the Association's Board of Directors, which was almost always drawn from the senior management at the largest member banks.[182]

Although Visa[183] and MasterCard[184] recently went public, becoming shareholder-owned companies, experts note that the reorganizations have not fundamentally changed the way they operate.[185] One scholar observed, MasterCard's and Visa's "post-IPO capital structure is designed to permit banks to retain effective control over the company without holding a majority of shares and giving a veneer of independence to decisions. . . ."[186]

---

178. *See* Martin, *supra* note 158; *see also* Pacheco & Sullivan, *supra* note 135.

179. *See* EVANS & SCHMALENSEE, *supra* note 57, at 63. The banks agreed to cooperate on setting operational standards, but to compete for merchants and cardholders. *Id.*

180. *Id.* at 162.

181. *Id*.

182. *Id*.

183. Katie Benner, *Visa IPO Prices at Record $17.9*, CNN MONEY (Mar. 18, 2008), http://money.cnn.com/2008/03/18/news/companies/visa_ipo.fortune/index.htm.

184. Tess Vigeland, *MasterCard IPO*, MARKETPLACE PUBLIC RADIO, May 3, 2006, http://marketplace.publicradio.org/display/web/2006/05/03/mastercard_ipo/.

185. EVANS & SCHMALENSEE, *supra* note 57, at 162.

186. Levitin, *Credit Card Fair Fee Act*, *supra* note 160.

Thus, the system, while not completely ignoring merchant and consumer interests,[187] tilts in favor of the banks and credit card companies because it was designed for them.[188] They can continue in that tradition today because they control the industry's infrastructure. They control PCI, hand down its rules, enforce them, impose fines, decide who to de-list, fix fees charged to merchants, and decide whether to impose higher PCI standards on breached companies. They essentially play the role of prosecutor, judge, and jury. Barring litigation, their decisions are final.

V. RECOMMENDATIONS FOR REFORM

Stemming credit card fraud requires federal intervention. The credit card companies and banks have weak incentives to crush the ability of criminals to infiltrate not just banks, but also merchants, large and small. The current go-it-alone approach may help secure an individual company or a defined group. Ultimately, however, it drives fraud to other, less protected businesses, since cyber criminals look "for easy pickings."[189] Therefore, we propose the enactment of a new federal law to direct the process of creating security standards that would tackle credit card fraud across the card industry.

A. MAKE SECURITY STANDARDS MANDATORY

We propose making security standards mandatory for all companies, regardless of size or type, that are involved in credit card transactions. Following the European Union model of having a public authority oversee the development of security rules and settle disputes,[190] we propose the appointment of a Data Security Commissioner ("Commissioner") to oversee the enactment of new

187. *Id.*

188. *See* EVANS & SCHMALENSEE, *supra* note 57, at 163.

189. *Zafar: Banks Need to Outsmart Criminals*, EURACTIV.COM (Jan. 31, 2010), http://www.euractiv.com/en/financial-services/zafar-banks-need-outsmart-criminals (last visited Aug. 16, 2010); *see also*, Gary Palgon, *Best Practices In Data Protection* (April 21, 2010), RETAILSOLUTIONSONLINE.COM, http://communications.retailsolutionsonline.com/article.mvc/Best-Practices-In-Data-Protection-0004 (describing cyber criminals as opportunists).

190. Council Directive 95/46/EC, art. 28, 1995 O.J. (L 281) 47, 48.

security standards.

B. LET STAKEHOLDERS DRAWN FROM THE INDUSTRY DESIGN THE SECURITY STANDARDS

The industry should design the security standards, as it is best situated to know its needs. However, to establish incentives to design the best system for all, on an industry-wide basis, the process should include all stakeholders, including merchants. Including all stakeholders is key to redressing the skewed incentives inherent in the industry's current lopsided power structure.

Therefore, we propose that a new Data Security Council ("Council") create industry standards and replace the one-sided PCI Executive Council. The new Council's membership would be drawn from groups across the industry: merchants of all sizes and sectors, payment processors, experts in security technologies, as well as banks and credit card companies. The associations representing the various parties, such as the American Bankers' Association and the National Federation of Retailers, would determine who should represent them on the Council. Our proposed Commissioner should also be a member of the Council.

This structure would allow for a representation of the industry's multi-faceted perspectives on security. Proposals for such multi-stakeholder dialogue have appeared in recent years. Examples include the United Nations Global Compact and the European Multi-Stakeholder Forum on Corporation Social Responsibility, "which propose dialogue among the different agents involved as a working methodology aimed at making headway in multilateral consensus proposals."[191]

C. LET THE COUNCIL GATHER INFORMATION

The Commissioner, in his or her position as a member of the Council, should have the power to compel companies to supply information about the type, extent, and costs of credit card fraud and related issues.[192] That information should be shared with the Council.

---

191. Laura Albareda et al., *Public Policies on Corporate Social Responsibility: The Role of Governments in Europe*, 74 J. BUS. ETHICS 391, 393 (2007).

192. This power follows a recommendation in the Durbin Amendment asking the Federal Reserve Bank to consider certain factors when drafting anti-fraud regulations related to debit cards. Consumer Financial Protection Act of 2010, Pub. L. No. 111-203

Appropriate information should be made public. Lack of accurate information about fraud undoubtedly contributed to the inertia about security in the industry. Raising awareness of the magnitude of fraud will help sustain the pressure for reform.

D. CUT INTERCHANGE FEES FOR COMPLIANT COMPANIES; DON'T FOR NONCOMPLIANT ONES

Security costs money. The smaller the company, the bigger the burden. Since the credit card companies own the card technology and they and the banks operate the networks, they would contribute the major investment in implementing standards. Small merchants would probably have to buy point of sale ("POS") machines to read whatever new cards the Council may propose. Larger merchants might additionally need to buy new software and hardware and integrate their networks with the new technology.

We propose giving merchants incentives to comply. For those merchants who are fully compliant with the new standards, the Commissioner would cap the interchange rate at a substantial discount of its current rate. For non-compliant merchants, interchange rates would be deregulated, with the banks and credit card companies free to charge what they wish. The goal would be to have a significant difference between the interchange rates for complaint and non-compliant firms. This would give merchants an immediate major financial benefit to becoming compliant. At the same time, investing in better security would lower merchants' own losses to fraud over the long-term.

Under this proposal, the banks and card companies would indirectly subsidize merchant compliance, since they would be receiving lower fees from compliant companies. However, this would be justified because they presumably would have less fraud to deal with as merchants become more secure.

The difference in interchange rates could also spawn entrepreneurs willing to lease POS systems to merchants for a fraction of the money they would save on interchange fees when becoming secure, making compliance even more affordable for certain retailers.

---

§§ 1075(a)(5)(B)(ii)(I)-(V), 124 Stat. 1376 (2010).

E. MAKE LYING ABOUT SECURITY COMPLIANCE A FELONY

The law would make it a felony for merchants to lie about whether they are security compliant and subject them to fines if they lie. Today, the consequences of lying about PCI compliance stand unclear. The new law needs to make them clear.

F. REDUCE THE ABILITY TO SHIFT FRAUD LOSSES DOWNSTREAM

The banks' use of loopholes in the wake of the Credit Card Act of 2009 suggests[193] that it would be difficult to reduce banks' ability to shift losses. However, their ability to shift losses is problematic only if the banks are the only entities responsible for setting the industry's security standards – because it weakens their desire to secure the system for all. However, under the new law, a Council represented by multiple stakeholders and overseen by a public Commissioner would set industry security standards. The standards would be mandatory and penalties would follow noncompliance.

It is time for the private sector, with the help of the public sector, to reconsider how to make our payment system safe from top to bottom. We hope that some of the suggestions herein might help move the system in that direction.

193. *See* Rodriguez, *supra* note 171, at 324-8.