Brooklyn Journal of Corporate, Financial & Commercial Law

Volume 5 | Issue 1 Article 1

2010

Private Disordering? Payment Card Fraud Liability Rules

Adam J. Levitin

ARTICLES

PRIVATE DISORDERING? PAYMENT CARD FRAUD LIABILITY RULES

Adam J. Levitin[*]

This Article argues that private ordering of fraud loss liability in payment card systems is likely to be socially inefficient because it does not reflect Coasean bargaining among payment card network participants. Instead, loss allocation rules are the result of the most powerful party in the system exercising its market power. Often loss liability is placed not on the least cost avoider of fraud, but on the most price inelastic party, even if that party has little or no ability to prevent or mitigate losses. Moreover, for virtually identical payment systems, there is international variation in both loss liability rules and security standards, suggesting that at least some variations are suboptimal.

True Coasean bargaining is not possible in payment systems; the transaction costs are too high because of the sheer number of participants. Targeted coordination and competition, however, can achieve outcomes that if not Coasean, are at least optimized relative to the current system. Thus, the Article suggests a pair of complimentary regulatory responses. First, regulators should develop a system for coordinating payment card security measures with governance that adequately represents all parties involved in payment card networks. And second, regulators should pursue more vigorous antitrust enforcement of card networks' restrictions on merchant pricing to expose the costs of participating in a payment system—which include fraud costs—to market discipline. The Article also presents an extended defense of the major existing regulatory intervention in payment card fraud loss allocation, the federal caps on consumer liability for unauthorized payment card transactions.

TABLE OF CONTENTS

---

[*] Associate Professor, Georgetown University Law Center. The author would like to thank William Bratton, Mark Budnitz, Robert Hunt, Sarah Levitin, and Ronald Mann for their comments and encouragement, and Steven Schwarzbach for research assistance. Comments? AJL53@law.georgetown.edu.

INTRODUCTION

Payment card fraud is a multi-billion dollar problem domestically and globally. While there are no firm numbers on the actual cost of payment fraud, one recent study estimates total costs of credit and debit card fraud in the U.S. at approximately $109 billion in 2008.[1] The losses from payment card fraud are borne directly by merchants, a range of financial institutions,

1. *See* LEXISNEXIS, 2009 LEXISNEXIS TRUE COSTS OF FRAUD STUDY 6, 50, 54 (2009), *available at* http://www.riskfinance.com/RFL/Merchant_Card_Fraud_files/LexisNexisTotalCost Fraud_09.pdf [hereinafter LEXISNEXIS FRAUD STUDY] (estimating total cost of all payment fraud in the U.S. at $191.30 billion and that credit and debit fraud account for 57% of the total). These figures should not be taken as precise statements because the study's methodology was not always clear and the figures did not include the costs sunk into fraud prevention by financial institutions and merchants or the non-pecuniary costs of fraud, such as distortions in consumer purchasing and payment patterns or time and hassle for consumers to straighten out credit reports and accounts. *See id.* at 17. For a *very* different estimate of fraud costs, see Richard J. Sullivan, *The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options,* FED. RESERVE BANK OF KANSAS CITY ECON. REV., 2Q 2010, at 101, 112, *available at* http://www.kansascityfed.org/ Publicat/Econrev/pdf/10q2Sullivan.pdf (estimating $3.718 billion in credit and debit card fraud losses in 2006 in the US). *See also* Kate Fitzgerald, *An Industry At A Loss*, PAYMENTSSOURCE, May 2010, at 16, 17 (reporting bank card fraud expenses as $.95 billion for 2009 and $1.11 billion for 2008).

and consumers. Payment card fraud also creates deadweight loss for the entire economy by increasing the cost of payments, the ultimate transaction cost.[2] Payment card fraud results in socialized losses because of the law enforcement resources spent combating the problem and may also frustrate some legitimate transactions that get caught by overly broad fraud prevention methods.[3]

The allocation of these losses occurs through a combination of public law and private ordering. Federal law generally limits individual consumer liability for unauthorized credit and debit card transactions to $50.[4] The liability of merchants and financial institutions as well as business cardholders[5] is generally determined through private ordering.[6]

The loss allocation rules are important not only because of their distributional consequences, but because of the incentives they create. The greater a party's liability for fraud losses, the greater incentive the party will have to take care to avoid fraud. As payment card fraud has (apparently) increased,[7] it is worth asking whether the current loss allocation system is the optimal one. Does it properly incentivize parties to take the optimal level of care from a social welfare standpoint? Does the loss allocation system facilitate or discourage commerce by limiting the transaction cost of payment?

---

2. To the extent that merchants bear losses, payment fraud may get passed on to consumers in the form of higher sale prices.

3. DELL INC., SUBMISSION OF DELL, INC. TO THE BOARD OF GOVERNORS OF THE FEDERAL RESERVE REGARDING SECTION 920 OF THE ELECTRONIC FUNDS TRANSFER ACT (REDACTED VERSION) 4, http://www.federalreserve.gov/newsevents/files/dell_comment_letter_20101118.pdf [hereinafter DELL LETTER].

4. 15 U.S.C. §§ 1643(a), 1693g(a) (2006); 12 C.F.R. § 226.12(b)(1)(ii) (2010) (credit cards); *id.* § 205.6(b) (debit cards). If the consumer does not provide the card issuer with timely notice that the consumer's card has been lost or stolen, the consumer's liability can increase up to $500. *Id.* See *infra* part IV for a more detailed discussion of consumer liability rules.

5. *See* 15 U.S.C. § 1603 (2006) (exempting "extensions of credit primarily for business, commercial, or agricultural purposes, or to government or governmental agencies or instrumentalities, or to organizations" from the credit transaction provisions of the Truth in Lending Act); *id.* § 1693a (defining "account" for the purposes of the Electronic Fund Transfer Act as being "established primarily for personal, family, or household purposes"). These exemptions would cover even sole proprietors if the credit was extended or the account established primarily for business purposes, as with a "business" card or "business" deposit account.

6. An exception is state laws relating to data security breach notification. *See* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 924–25, 972–84 (2007).

7. LEXISNEXIS FRAUD STUDY, *supra* note 1, at 26–27. Given the lack of solid payment card fraud statistics in the United States, it is impossible to say with absolute certainty whether fraud levels are increasing, much less relative to the size of the market. While issuers report fraud losses, some of these losses are first-party fraud, where the consumer simply denies having carried out the transaction that he or she made, while others are third-party fraud. Jasbir Anand, *First Party Fraud*, SC MAGAZINE (Apr. 1, 2008), http://www.scmagazineus.com/first-party-fraud/article/108545.

There is a sizeable literature on fraud and mistake liability allocation rules in payments systems.[8] This literature, however, generally focuses on public law and on the propriety of liability allocation to consumers. There has been little scholarly consideration of the private law that allocates liability between merchants and financial institutions.[9] The reason for this comparative neglect is unclear. Until recently, payment card network operating rules were not publicly available, which limited a critical primary source for scholars. Moreover, scholars may have considered the allocation of liability between merchants and financial institutions less of a policy concern because the asymmetries in terms of information, sophistication, and ability to exercise rights are less acute between merchants and financial institutions than they are between consumers and financial institutions.

In perhaps the most extensive exposition on the issue, Professor Richard Epstein and attorney Thomas Brown argue that the current system of private loss allocation layered on top of a statutory baseline is flawed.[10] Epstein and Brown argue that losses should be allocated solely through private ordering. In their view, which they "would have thought beyond

---

8. *See* Mark E. Budnitz, *Commentary: Technology as the Driver of Payment System Rules: Will Consumers Be Provided Seatbelts and Air Bags?*, 83 CHI.-KENT L. REV. 909 (2008); Robert D. Cooter & Edward L. Rubin, *A Theory of Loss Allocation for Consumer Payments*, 66 TEX. L. REV. 63, 71–72 n.42 (1987) (reviewing pre-1970s writings on this topic); Francis J. Facciolo, *Unauthorized Payment Transactions and Who Should Bear the Losses*, 83 CHI.-KENT L. REV. 605 (2008); Clayton P. Gillette, *Rules, Standards, and Precautions in Payment Systems*, 82 VA. L. REV. 181 (1996); Clayton P. Gillette & Steven D. Walt, *Uniformity and Diversity in Payment Systems*, 83 CHI.-KENT L. REV. 499 (2008); Gail Hillebrand, *Before the Grand Rethinking: Five Things To Do Today with Payments Law and Ten Principles to Guide New Payments Products and New Payments Law*, 83 CHI.-KENT L. REV. 769 (2008); Sarah Jane Hughes, *Duty Issues in the Ever-Changing World of Payments Processing: Is It Time for New Rules?*, 83 CHI.-KENT L. REV. 721 (2008); Ronald J. Mann, *Credit Cards and Debit Cards in the United States and Japan,* 55 VAND. L. REV. 1055 (2002) [hereinafter Mann, *Credit Cards and Debit Cards*]; Ronald J. Mann, *Making Sense of Payments Policy in the Information Age*, 93 GEO. L.J. 633 (2005) [hereinafter Mann, *Making Sense of Payments*]; James Steven Rogers, *The Basic Principle of Loss Allocation for Unauthorized Checks*, 39 WAKE FOREST L. REV. 453 (2004); Linda J. Rusch, *Reimagining Payment Systems: Allocation of Risk for Unauthorized Payment Inception*, 83 CHI.-KENT L. REV. 561 (2008).

9. I have identified only two works that focus on this issue in any detail. *See* Duncan B. Douglass, *An Examination of the Fraud Liability Shift in Consumer Card-Based Payment Systems*, FED. RES. BANK OF CHI. ECON. PERSP., 1Q 2009, at 43; Richard A. Epstein & Thomas P. Brown, *Cybersecurity in the Payment Card Industry*, 75 U. CHI. L. REV. 203 (2008). Some other works touch on payment card fraud liability rules, but do not consider them in detail, as they focus on other types of payment systems. *See* Robert G. Ballen & Thomas A. Fox, *The Role of Private Sector Payment Rules and a Proposed Approach for Evaluating Future Changes to Payments Law*, 83 CHI.-KENT L. REV. 937 (2008) (focusing on payment transaction rules among financial institutions); Facciolo, *supra* note 8 (including a review of checks, ACH debits and wire transfers along with credit and debit cards); Mann, *Credit Cards and Debit Cards, supra* note 8; Rusch, *supra* note 8 (focusing on risk-allocation in unauthorized debits from deposit accounts).

10. Epstein & Brown, *supra* note 9, at 209. Epstein and Brown approach payment systems with a very strong set of anti-regulatory priors, or, as they refer to it, as their "classical liberal perspective." *Id.* at 203. Brown, an antitrust attorney, has previously worked in-house for Visa. *Id.* at n. ††.

reproach . . . voluntary contracts offer by far the best way to allocate the risks of loss, and the duties of prevention, among the various parties within this elaborate network."[11] Thus, Epstein and Brown "see no reason even for th[e] (modest) restriction on freedom of contract [created by the federal limitation on consumer liability for unauthorized transactions]. If payment card companies think larger penalties are appropriate and disclose such penalties to consumers, the losses should not be socialized as a matter of law."[12] For Epstein and Brown, all liability for unauthorized transactions should be allocated contractually; mandatory (or even default) statutory rules are inappropriate in their view.[13]

This Article argues that we should be skeptical of the efficiency of private ordering in payment card markets. In a world with a complete set of perfectly competitive markets, private ordering is surely the right outcome—Coasean bargaining would ensure that fraud losses would be allocated to the least cost avoider and the optimal level of care would ensue. But there is never a complete set of perfectly competitive markets except in economists' models and dogmatic fantasies,[14] and Coase's great lesson is that transaction costs matter; in their presence, the initial allocation of liability is critical.[15]

Payment card markets are always incomplete, as there are no futures or insurance markets in most areas of payments through which risks can be hedged.[16] If one commits to using a payment system, thereby incurring fraud risk, one cannot also short payment fraud futures as a hedge, much less the futures on a particular card or transaction. At best, one could short a payment card network, but that is an imperfect proxy for fraud risk, as the costs to a network from elevated fraud are limited, and is hardly negatively correlated with fraudulent activity on a particular card-linked account.[17] Payment card markets are also imperfect because of limited information. For example, it is often impossible to determine how a fraud was perpetrated and therefore who would have been the least cost avoider.

Epstein and Brown assume something close to a perfect market in payment systems, noting the "high level of competition that exists everywhere in the credit card industry."[18] Market realities are quite

---

11. *Id.* at 209.

12. *Id.* at 219.

13. *See id.* at 209, 219, 223. It is unclear whether Epstein and Brown would envisage payment card companies actually bargaining with individual consumers or whether they would simply present consumers with contracts of adhesion in which fraud loss rules were one of many non-negotiable components of a package offer.

14. *See* JOSEPH E. STIGLITZ, WHITHER SOCIALISM? 27–44 (1994) (presenting a critique of the first fundamental theorem of welfare economics).

15. R. H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 14–15 (1960).

16. *See generally* Mark D. Flood, *An Introduction to Complete Markets*, FED. RES. BANK OF ST. LOUIS REV., Mar.-Apr. 1991, at 32 (explaining incomplete markets, futures, and hedged risks).

17. *See generally* LEXISNEXIS FRAUD STUDY, *supra* note 1.

18. Epstein & Brown, *supra* note 9, at 203.

different.[19] Some parts of payment cards markets are intensely competitive, while others are not.[20] Payment card networks—MasterCard, Visa, Amex, Discover, and around a dozen relatively small personal-identification-number (PIN)-debit networks—are two-sided networks.[21] Network effects, combined with the need to roll out payment networks nationally, at the very least, create high barriers to entry for new networks.[22] Further, while there are numerous card issuers and acquirers, the market is heavily concentrated in a handful of institutions. The five (ten) largest card issuers account for 74% (90%) of the credit card market and 43% (51%) of the debit card market in terms of purchase volume.[23] More critically, the mere fact that there are numerous competitors does not mean that there is competition along every axis of the market. For example, competition may exist for market share or for price, but not for security.

Payment card systems also involve a variety of participants with divergent incentives. This creates intense coordination problems. The networks lead the coordination efforts, but they are driven by their own incentives, primarily to increase the size of the network.[24] As long as fraud remains sufficiently low that it does not damage the network's reputation, the network's primary concern is maximizing total transaction volume, irrespective of whether the transactions are fraudulent.[25] Increasing the size of the network is a function of calibrating the network's cost allocation (including fraud) to fully leverage network participants' price elasticity.[26]

Fraud liability is a cost of using a payment system and is therefore a type of pricing affected by the level of competition in the market. Therefore, more price inelastic participants (those whose demand for a payment system's services is the least sensitive to price changes) might bear a larger share of fraud losses, regardless of whether they are the least cost avoiders of the fraud. By allocating fraud losses to the most price inelastic

---

19. *See* Adam J. Levitin, *Priceless? The Economic Costs of Credit Card Merchant Restraints*, 55 UCLA L. REV. 1321, 1356–63 (2008) [hereinafter Levitin, *Economic Costs*].

20. *Id.*

21. *Id.* at 1387.

22. *Id.* at 1386–87; *see also* JOHN M. GALLAUGHER, INFORMATION SYSTEMS: A MANAGER'S GUIDE TO HARNESSING TECHNOLOGY (2010), *available at* http://www.flatworldknowledge.com/pub/1.0/information-systems-manager%E2%80%99s-/206326#web-206326.

23. *See* THE NILSON REP. ISSUE 919 (Feb. 2009); THE NILSON REP. ISSUE 918 (Jan. 2009); THE NILSON REP. ISSUE 917 (Jan. 2009); Adam J. Levitin, *Interchange Regulation: Implications for Credit Unions*, FILENE RESEARCH INST., Nov. 24, 2010, at 1, 39, http://www.federalreserve.gov/newsevents/files/levitin_filene_paper.pdf.

24. *See generally* Levitin, *Economic Costs*, *supra* note 19, at 1356–59, 1364–65, 1398 (detailing ways that networks coordinate their systems to raise revenue and discussing the negative network effect of negative externality).

25. *See generally* David Charny, *Nonlegal Sanctions in Commercial Relationships*, 104 HARV. L. REV. 373, 393 (1990) (discussing the nonlegal sanction of loss of reputation among market participants); Schwartz & Janger, *supra* note 6, at 929–32 (discussing the cost and associated pressures of reputational sanctions).

26. *See* Levitin, *Economic Costs*, *supra* note 19, at 1364–66.

party, the number of network participants is maximized, but deadweight loss may occur if the most price inelastic network participant is not also the least cost avoider of fraud.

Previous work on payment systems has viewed fraud liability rules as unconnected with competition issues.[27] Thus, in their groundbreaking paper on the economics of payment system loss allocation rules, written well before the emergence of major payment card antitrust litigation, Professors Robert D. Cooter and Edward L. Rubin noted that "[t]he structure of the financial services industry may cause market failures, such as oligopolistic or monopolistic behavior, but these tend to affect pricing rather than loss allocation."[28] Ironically, though, one of the sources Cooter and Rubin cited for this was the seminal paper on credit card interchange fee competition.[29] While Cooter and Rubin viewed loss allocation as a distinct issue from pricing, a major point of this Article is that loss allocation is itself a type of pricing and cannot be viewed as unaffected by antitrust matters.

This Article argues that the rules for allocating payment card fraud loss are likely to be suboptimal because they are shaped by discrepancies in market participants' bargaining power. In payment card networks there is not unfettered bargaining over fraud loss allocation. Instead of Coasean bargaining, there is merely fiat ordering by the most powerful party in the network—the network association itself—which is interested in maximizing total transaction volume, rather than total nonfraudulent transaction volume.[30] In such circumstances, we should be skeptical that private ordering achieves socially efficient outcomes. Instead, in a market replete with competition and information problems, private *dis*ordering may obtain, and, with it, negative social externalities.

To this end, the Article reviews payment card network fraud liability allocation rules, focusing on Visa and MasterCard, the two largest payment card issuers that, combined, accounted for 84% of the total U.S. payment card (debit, credit, and prepaid) market in purchase transaction volume in 2008.[31] It shows that liability allocations among card network participants are likely inefficient as they often place liability on parties with little or no ability to prevent fraud.[32] The Article also notes international variation in liability rules and security measures, and the fraud arbitrage problems that stem from these variations. International inconsistency in liability rules and

---

27. Professor Ronald Mann has recognized this point implicitly in his comparative study of credit cards in the United States and Japan. *See* Mann, *Credit Cards and Debit Cards*, *supra* note 8, at 1088–99 (discussing impact of fraud rates on merchant fees).

28. Cooter & Rubin, *supra* note 8, at 68 n.30.

29. *See id.* (citing William Baxter, *Bank Interchange of Transactional Paper: Legal and Economic Perspectives,* 26 J.L. & ECON. 541, 554–55, 586–88 (1983)).

30. *See* Levitin, *Economic Costs*, *supra* note 19, at 1334–38.

31. THE NILSON REP. ISSUE 924, at 8 (Apr. 2009) (comparing 2008 "Totals" for Visa and Mastercard "Credit" and "Debit & Prepaid" categories against 2008 "Credit & Debit Totals").

32. *See* Douglass, *supra* note 9, at 46–47.

security measures for the same companies in virtually identical markets suggests that private ordering may not be producing optimal results globally.[33]

While private ordering may not produce optimal results, regulatory intervention poses its own problems. Regulators are subject to their own idiosyncratic concerns and pressures, and they also lack perfect information.[34] Yet, if regulatory intervention cannot achieve optimal outcomes, it might still help optimize market outcomes. Thoughtful regulatory intervention can compensate for some of the bargaining power disparities and help achieve an outcome that is closer to that which would obtain in a complete, perfectly competitive market.

Accordingly, this Article argues for two complimentary regulatory interventions. First, broader-based payment card security measure coordination should be encouraged. The current coordination mechanism for payment card security—the Payment Card Industry Security Standards Council—features a governance structure that does not adequately represent all interests in payment card networks or provide them with due process. As a result, the Council is perceived as being an instrumentality for the card networks to reinforce the placement of liability on the most price inelastic type of network participant, rather than engaging in effective reforms. To this end, it might be necessary for payment card security coordination to be conducted under a federal aegis.[35]

Second, card networks should be encouraged to compete more vigorously for merchants, be this through legislation or rulemaking or through antitrust enforcement of payment card network rules pertaining to merchant pricing.[36] Fraud costs are part of pricing.[37] While the huge transaction costs in coordinating multiple parties in payment card networks defeats true Coasean bargaining, better price competition among networks for merchants will help achieve a result closer to the Coasean ideal.

The Article also presents a defense of the federal limitation on consumer liability.[38] The federal limitation creates a moral hazard and constrains the range of potential bargaining.[39] It is tempered, however,

---

33. *See infra* pp. 22–30.

34. Once we accept that the market is flawed, however, there is no inherent reason to favor market solutions over regulatory ones. Both systems might produce suboptimal outcomes, and we have no way of ascertaining which system is more likely to do so or whether an outcome is in fact optimal. In such circumstances, there is no good reason to fall back on anti-regulatory priors. Instead, when efficiency proves an indeterminate metric, it must be jettisoned for a metric, such as political accountability.

35. *See infra* pp. 30–32.

36. *See infra* pp. 32–36.

37. *See* Gillete & Walt, *supra* note 8, at 500; Adam J. Levitin, *The Antitrust Super Bowl: America's Payment Systems, No-Surcharge Rules, and the Hidden Costs of Credit*, 3 BERK. BUS. L.J. 265, 273–74 (2005).

38. *See infra* Part IV.

39. Douglass, *supra* note 9, at 46.

through monetary and nonmonetary deductibles and copayments and reflects a reasonable response to an adverse selection problem and to the enormous informational and bargaining cost asymmetries between consumers and card issuers regarding fraud risk, as well as to consumers' limited ability to prevent most third-party fraud and limited ability to bear losses relative to other payment card network participants.

This Article proceeds as follows. Part I provides an overview of the structure of payment card networks and their loss allocation rules in the United States. Part II questions whether the liability rules do in fact result in a Kaldor-Hicks efficient outcome. Part III considers possible and existing regulatory interventions to level the playing field and move payment card networks closer to Coasean bargaining outcomes. Part IV examines the consumer loss liability rules and presents a defense of the federal limitations on consumer liability of unauthorized transactions.

An important introductory note: this Article focuses solely on the issue of allocation of losses for unauthorized transactions. It does not generally address the related issues of liability for compromised payment data storage or data transmission that results in fraud losses for others. Data security breaches have become a major issue in payment card security in recent years. Whether there should be some form of tort liability for data security breaches, whether liability should be set by private ordering, what the liability standard should be, and whether compliance with industry standards such as Payment Card Industry Data Security Standard would be sufficient to relieve liability are important questions.[40]

Ultimately, however, flaws in data storage or data transmission only matter to the extent that unauthorized transactions can occur. The data have no inherent value; the data's attraction to fraudsters derives solely from their ability to capitalize on it, and using it for fraudulent transactions is the most immediate way to do so.[41] Thus, data breach liability is better conceived as liability for *potential* fraud and the steps that must be taken to reduce the likelihood that the breach will translate into fraud, such as reissuance of cards with new numbers following a breach. It is also often difficult to trace the unauthorized use of a card to a particular data security breach, which makes the liability relationship more tenuous.[42] To be sure, there are improvements that can and should be made in data storage and transmission—tokenization and end-to-end encryption should both be pursued vigorously.[43] But those improvements will not eliminate fraud

40. *Cf.* The T.J. Hooper, 60 F.2d 737, 740 (2d Cir. 1932) (Hand, J.) (suggesting that industry standard is not necessarily the proper standard of diligence as "a whole calling may have unduly lagged in the adoption of new and available devices").

41. Not all data breach issues even relate to payments, although payment data is the most readily monetizable type of data.

42. Sullivan, *supra* note 1, at 108, 110.

43. Tokenization is a data fortification strategy. It is meant to address the problem of data residing in relatively vulnerable locations, such as with retailers. Tokenization means that data

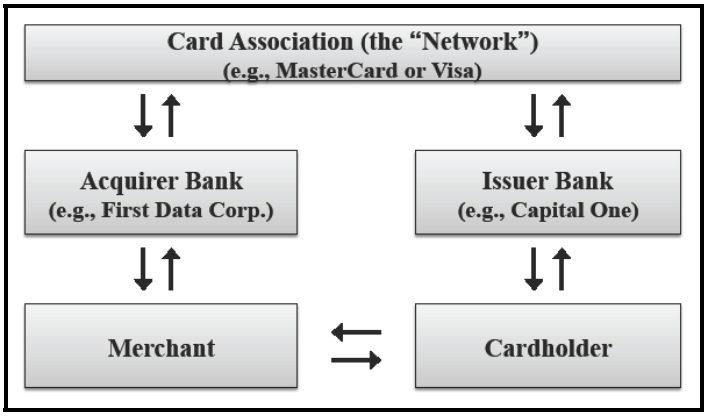
problems. Better data protection will make it harder to get the data necessary to commit certain types of fraud, but the critical line of fraud defense for all third-party fraud is transaction authorization.

I. PAYMENT CARD NETWORKS AND LIABILITY RULES

A. STRUCTURE OF PAYMENT CARD NETWORKS

Payment card transactions all involve multi-party networks of financial institutions, consumers, and merchants. Transmission of a payment from a consumer to a merchant to pay for goods or services is conducted through at least three financial institutions: the consumer's bank (the issuer bank), the merchant's bank (the acquirer bank), and the card network association (MasterCard, Visa, Amex, Discover, or PIN debit network) that intermediates between the banks and sets the rules governing their transactions. Thus, a payment card transaction involves at least five parties, although in the case of American Express and Discover,[44] the card network is often also the card issuer and the acquirer. (See Figure 1).

Figure 1. Payment Card Network Structure



Often a payment card transaction involves additional parties. Acquirers frequently outsource all but the financing element of their operations. The task of recruiting merchant customers for the acquirer is often outsourced to an independent sales organization (ISO), and all the technical linkages between the merchant and the card network association are often outsourced

resides in harder-to-hack "fortified" locations; merchants would only retain a "token" number that links to the data stored off-site. Instead of residing with merchants, who do not specialize in data security, tokenization moves the data to companies with expertise and reputational capital (and potentially insurance policies) that guarantee data protection. End-to-end encryption means that card data is never transmitted in an unencrypted form.

44. Levitin, *Economic Costs*, *supra* note 19, at 1328.

to a separate data processor.[45] For Internet transactions a separate gateway provider might also be involved.[46]

In a payment card transaction, the consumer must first transfer information about the consumer's account (either funded or a line of credit) to the merchant, or more precisely, to the merchant's acquirer or data processor. This can be done in several ways. The information can be transferred electronically via a magnetic swipe. The information can be transferred electronically via radio-frequency identity (RFID) chip ("contactless"). The information can be transferred physically via an impression made by an imprinter (a "knucklebuster"). The information can be transferred orally and recorded by hand. The information can be transferred in a written form, as occurs in mail-order transactions. Or the information can be transferred electronically via a Web site. Some transactions require additional information (such as a PIN number or a ZIP code) to be conveyed via a PIN pad.

Once this information is conveyed to the merchant, it is then relayed to the credit card network by the merchant's processor for authorization, capture, and settlement (ACS).[47] Authorization involves the *card network* first verifying that the card is real and then the *issuer* approving the transaction. Once a transaction has been authorized, it may then be captured.

Capture involves the transfer of funds from the issuer bank to the acquirer bank. The transfer is done between the institutions' accounts at the card network association, which serves as a clearinghouse for the payments.[48] The issuer transfers to the acquirer the amount of the transaction minus a fee, known as the interchange fee.[49] The interchange fee is set by the network and varies by the type and size of the merchant, the type of card (consumer or commercial, credit or debit), and the level of rewards on the card.[50] The card network also takes out various fees to cover its costs of processing the transaction plus its profit margin.[51] Thus, the network debits the issuer's account for the amount of the transaction less

---

45. *See* Ramon P. DeGennaro, *Merchant Acquirers and Payment Card Processors: A Look Inside the Black Box*, FED. RES. BANK ATLANTA ECON. REV., 1Q 2006, at 27, 31.

46. Adam J. Levitin, *Priceless? The Social Costs of Credit Card Merchant Restraints*, 45 HARV. J. ON LEGIS. 1, 5 n. 13 (2008) [hereinafter Levitin, *Social Costs*].

47. Sometimes the merchant never actually has control over the data, which instead goes straight to the processor.

48. DeGennaro, *supra* note 45, at 33.

49. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-08-558, CREDIT AND DEBIT CARDS: FEDERAL ENTITIES ARE TAKING ACTIONS TO LIMIT THEIR INTERCHANGE FEES, BUT ADDITIONAL REVENUE COLLECTION COST SAVINGS MAY EXIST 1 (2008).

50. *See* Levitin, *Economic Costs*, *supra* note 19, at 1333.

51. Historically, MasterCard and Visa were mutual organizations owned by their member institutions. Accordingly, they only charged a "switch" fee to cover their costs of processing transactions. Since becoming publicly-traded stock companies, however, MasterCard and Visa have needed to operate on a for-profit basis and have added additional fees.

the interchange fee and credits the acquirer bank's account for the transaction amount minus both interchange and network fees.

Finally, the transaction is settled, meaning that the acquirer credits the merchant's account with the funds representing the transaction amount minus its own fee, called the merchant discount fee. The merchant discount fee is set to cover the interchange fee and network fees paid by the acquirer, as well as the acquirers' other costs and a profit margin. Frequently the merchant discount fee is explicitly priced as "interchange plus"—as a spread over the applicable interchange and network fees—making interchange and network fees functionally pass-thru fees to the merchant.[52]

When a transaction is reversed (referred to as a "chargeback"), the system works backwards.[53] The acquirer transfers funds from the merchant's account to its account and then to the network. These funds are captured in the issuer's account. The issuer then settles the funds back in the consumer's account. Chargebacks generally involve their own set of additional fees from the network to the acquirer and thence from the acquirer to the merchant.[54] The interchange and network fees on the original transaction are not always refunded to the merchant when there is a chargeback.[55]

Payment card networks are "two-sided networks,"[56] meaning that they have two distinct types of end customers: merchants and consumers. Payment card networks are unique among two-sided networks, however, in that they have not only two different types of end customers, but also two different types of intermediate customers: acquirers and issuers. The existence of these four different types of customers significantly complicates the economic workings of payment card networks.

In a two-sided network, the value of participating in the network to one type of customer depends on how many of the other type of customer are participating. For example, heterosexual bars and newspaper classifieds are both examples of two-sided networks. At heterosexual bars, the appeal of

---

52. Interchange Reimbursement Fees, MERCHANT COUNCIL, http://www.merchantcouncil.org/merchant-account-information/rates-fees.php (last visited Oct. 16, 2010). A "blended rate" that gives merchants a single merchant discount rate, regardless of the particular mix of interchange rates on the cards used, is a common alternative, especially for smaller merchants. *Id.* (Enhanced Recover Reducer (ERR)).

53. Chargebacks & Dispute Resolution: Chargeback Cycle, VISA, http://usa.visa.com/merchants/operations/chargebacks_dispute_resolution/chargeback_cycle.html (last visited Oct. 16, 2010).

54. Merchant Card Processing: Frequently Asked Questions, BANK OF AMERICA, http://www.bankofamerica.com/small_business/merchant_card_processing/index.cfm?template=faqs#cb_2 (last visited Oct. 16, 2010).

55. *See generally* MASTERCARD WORLDWIDE, CHARGEBACK GUIDE (Apr. 16, 2010) [hereinafter MASTERCARD CHARGEBACK GUIDE].

56. *But see* Dennis W. Carlton & Alan S. Frankel, *Transaction Costs, Externalities, and "Two-Sided" Payment Markets*, 2005 COLUM. BUS. L. REV. 617, 626–31 (arguing that the concept of two-sided markets is insufficiently defined and that most markets can be described as two-sided because consumers benefit from the supply created in response to the demand of other consumers).

the bar to men depends on the number of women present and vice-versa. Straight men do not want to go to bars populated only by other straight men, and straight women do not want to go to bars populated only by other straight women. Likewise, newspaper classifieds are of interest to advertisers based on the number of readers and to readers based on the number of advertisers. Advertisers want classified readers and classified readers want advertisers. Similarly, the value of being a cardholder in a payment card network depends on the number of merchants in the network and vice-versa.

In card networks, as with other two-sided networks, the increase in marginal value from greater network participation diminishes as the network grows. It is of little consequence to a consumer if a card network has 50 million or 50 million and one merchants in the network. Once a network is sufficiently well established, its marginal size is of limited importance to its value to its participants.

A multi-bank payment card network like MasterCard or Visa (and American Express and Discover for their third-party issuers) has a more delicate balancing act to maintain than simply achieving a balance between the two types of end-users, consumers and merchants. Multi-bank networks also have to ensure participation of a sufficient number of both issuers and acquirers in order to ultimately optimize and grow end-user participation.[57]

The existence of both intermediate customers and end-customers for payment card networks further complicates the dependency. The value of a network to the intermediate customers—issuers and acquirers—depends not on the number of the other type of intermediate customer, but on the number of the other type of intermediate customer's end-customer. Acquirers care about the number of cardholders in the network, and issuers care about the number of merchants.[58] This is not the case for the end-customers. It is irrelevant to consumers and merchants how many intermediate customers (issuers and acquirers) are in the network;[59] instead, network value depends on the numerosity (and geographic and industry concentration) of the other type of end-customer.[60]

Price elasticities—willingness to pay—for network services are likely to differ between customer types in a two-sided network. Because the value of the network to its participants depends on increasing the size of both sides of the network, pricing of access to the network involves allocating network costs to the different types of participants according to their price elasticity in order to maximize the size, and hence value, of the network.[61]

---

57. *See id.* at 631–37.

58. *See* Levitin, *Economic Costs*, *supra* note 19, at 1377.

59. Consumers care about the number of issuers of cards in general, but for reasons related to competition for card provision, rather than network dynamics.

60. *See* Levitin, *Economic Costs*, *supra* note 19, at 1364–65.

61. *Id.*

A central role of the network association is to coordinate optimal participation in the network through price manipulation, both in terms of direct monetary pricing and indirect pricing through network rules that impose liability on network participants for losses or limit network participants' ability to reallocate costs to other network participants.[62]

For merchants, these costs are the merchant discount fee, any sunk equipment fees, and fees to ISOs and processors, as well as the costs of fraud. For consumers using a credit card, these costs are an annual fee (if any), the costs of revolving a balance, ancillary fees (over-limit, late, cash advance, foreign transaction, e.g.), and the costs of fraud.[63] For consumers using a debit card, the costs are account maintenance fees (if any), overdraft fees (if any), and the costs of fraud. For merchants and consumers, fraud costs are part of the total cost of participating in a payment card network. Fraud liability is a price component, just not one that is explicitly priced.

Payment card network associations do not have contractual privity with the end-users of the networks.[64] Accordingly, they do not have direct control over the total price for the end-users. They may exercise this control only indirectly through their pricing and rules for issuers and acquirers. These prices and rules set a floor for the pricing and rules that issuers and acquirers apply to their respective end-users, consumers, and merchants. While the payment card networks' rules technically bind only the card networks' member institutions—issuer and acquirer banks—the costs are passed on to the end-users to the extent permitted by law (and card association rules).[65]

B. PAYMENT CARD LIABILITY RULES IN THE UNITED STATES

In the United States, the liability for unauthorized payment card transactions is allocated partially by statute and partially by private ordering. Federal law generally limits individual consumer liability for unauthorized transactions to $50 for credit and debit cards, albeit with important exceptions discussed in Part IV, *infra*.[66] The liability of merchants and financial institutions is determined through private ordering under payment card network rules. The payment card networks' rules technically bind only the card networks' member institutions—issuer and acquirer banks. Acquirers, however, uniformly pass on their liability to their merchants by contract, sometimes adding fees.

---

62. *Id.* at 1334–38 (describing network rules that restrict merchants' ability to reallocate costs to consumers).

63. Consumers bear the cost of interchange indirectly in the form of higher prices or reduced merchant services. *See* Levitin, *Social Costs*, *supra* note 46, at 27–37.

64. *See* Levitin, *Economic Costs*, *supra* note 19, at 1327–31.

65. *See id.* at 1334–39.

66. *See supra* note 4.

All payment card networks have substantially identical rules,[67] although there is variation in the often inscrutable details. In certain circumstances, the issuer is allowed to chargeback the transaction to the acquirer, thereby putting loss liability on the acquirer.[68] The card networks' rules governing chargebacks are extremely complicated and run hundreds of pages long, but they can largely be summarized as follows: for card-present transactions, where the merchant can physically examine the card and obtain a signature or PIN code, the issuer bears all liability for unauthorized transactions, provided that the merchant followed the required security steps. These steps generally involve inspection of the card, obtaining authorization from the issuer for the transaction, and obtaining a signature from the cardholder.[69] Signatures, as we shall see, are not authorization devices, but ex post loss allocation devices. Card-present transactions include any transaction in which the card is physically swiped at a magnetic stripe (mag stripe) reader in the presence of the merchant's employee, and is imprinted on a "knucklebuster" or otherwise physically handled by the merchant. Some networks also include small ticket ("No Signature Required") transactions and contactless or "proximity" RFID transactions in this category.[70] For card-not-present (CNP) transactions, such as mail-order and telephone-order (MOTO) or Internet transactions, the acquirer (and hence the merchant) bears all liability for unauthorized transactions.[71]

---

67. *See* MASTERCARD WORLDWIDE, MASTERCARD RULES (May 12, 2010) [hereinafter MASTERCARD RULES]; VISA, INT'L OPERATING REGULATIONS (Apr. 1, 2010) [hereinafter VISA INT'L REGULATIONS]; AMERICAN EXPRESS, MERCH. REGULATIONS—U.S. (Apr. 2010); DISCOVER, MERCHANT OPERATING REGULATIONS, RELEASE 10.2 (Apr. 16, 2010) [hereinafter DISCOVER MERCHANT OPERATING REGULATIONS].

68. *See, e.g.*, VISA, INT'L OPERATING REGULATIONS—DISPUTE RESOLUTION PROCEDURES 20 (Nov. 2, 2009), *available at* http://usa.visa.com/download/merchants/visa-international-operating-regulations-dispute-resolution-rules.pdf [hereinafter VISA DISPUTE PROCEDURES].

69. *Id.* at 100–02. Gas station pump transactions, which require a physical card to be swiped, do not qualify as "card-present" because there is no physical examination of the card by a station employee.

70. *See id.* at 102–03; AMERICAN EXPRESS, MERCH. REGULATIONS—U.S. (Oct. 2009) § 4.6.2., at 31. The shifting of fraud liability from merchants to issuers for these types of transactions is to foster merchant acceptance of contactless and signature-free transactions, which issuers might anticipate resulting in larger ticket transactions because of the seamlessness of the spending process.

71. VISA DISPUTE PROCEDURES, *supra* note 68, at 112–13. There are some important exceptions to this rule. For example Visa puts the loss on the issuer if the merchant shipped merchandise and the issuer did not participate in its Address Verification Service. *Id.* at 114–15.

II. WHAT HATH PRIVATE ORDERING WROUGHT?

A. WHO IS THE LEAST COST AVOIDER? CARD-PRESENT TRANSACTIONS

In a world of perfect markets, liability for a harm is optimally allocated to the least cost avoider of that harm.[72] The fact that payment cards are two-sided networks is irrelevant to the application of the least cost avoider principle; allocating the loss to the least cost avoider is the efficient outcome, regardless of varying price elasticities between merchants and card issuers. This can be seen from considering how the total value of a payment system to its participants varies with fraud loss allocation. The total value (V) of a payment system to its participants is equal to their collective net benefit from the system excluding fraud costs (E) minus fraud costs (F). Thus, $V=E-F$. We can refine this as $V=E_{Merchant}+E_{Bank}-F_{Merchant}-F_{Bank}$.

The values of $F_{Merchant}$ and F_{Bank} depend on which party is liable for fraud. If a party is not liable, then its fraud costs are zero. For simplicity's sake, assume that fraud costs can either be allocated wholly to the merchant or wholly to the issuer bank, but not shared. Therefore, if the costs are allocated wholly to the merchant, $F_{Bank}= 0$, and if the costs are allocated wholly to the card issuer, then $F_{Merchant}=0$.

Thus, the value maximizing proposition depends on whether $E_{Merchant}+E_{Bank}-F_{Merchant} >?< E_{Merchant}+E_{Bank}-F_{Bank}$, which means it depends on whether the issuer bank and the merchant are liable, $F_{Bank}>?<F_{Merchant}$. The relative values of F_{Bank} and $F_{Merchant}$ depend on how cheaply each party can avoid fraud, as F, the total costs of fraud, is the sum of fraud losses plus fraud avoidance expenses. If the merchant can avoid fraud more cheaply then the issuer bank, then $F_{Bank}>F_{Merchant}$, and V will be maximized by placing liability on the merchant, whereas if the issuer bank can avoid fraud more cheaply, then $F_{Bank}<F_{Merchant}$, and V will be maximized by placing liability on the issuer bank.

The key point to see here is that E is irrelevant to the outcome. E is the net benefit that the network's participants derive from participating (excluding fraud costs). The participants' maximum willingness to pay in the absence of fraud costs—the limit to their price elasticity—must equal E, as they will not pay beyond the net benefit received. This means that the network participants' price elasticity is irrelevant for the application of the least cost avoider principle. Even in a two-sided network, then, the least cost avoider principle is unaltered.

---

72. *See, e.g.*, GUIDO CALABRESI, THE COST OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS 136–38 (1970) (exploring the least cost avoider in a typical car and pedestrian accident).

So, are fraud losses in payment card networks allocated to the least cost avoider? Are the card networks' fraud loss allocation rules efficient?

For card-present transactions, the rules place the loss on the issuer, unless the merchant has failed to follow some basic steps in inspecting the card and obtaining a signature or PIN (with exceptions for proximity and no-signature small ticket transactions).[73] Consider how this allocation applies in the five basic card-present fraud situations:[74]

1. The "friendly fraud" or "first-party fraud" scenario, when a real cardholder uses his or her card to obtain goods or services and then denies having authorized the transaction or otherwise claims that the transaction was defective (by claiming nondelivery of goods or nonconforming merchandise, e.g.).
2. The "stolen card" scenario, when a card is stolen and used by the thief (or a taker from the thief) to perform a transaction. The card is a real card being used by an unauthorized user.
3. The "fraudulent issuance" scenario, when a transaction is performed on a real card that was issued based on fraudulent information (typically to a fictitious individual). The card is a real card being used by an authorized (but fake) user.
4. The "real account, counterfeit card" scenario, where the transaction is performed using a counterfeit card that uses real data copied from an actual card. The card is a fake card, but the user is an authorized user.
5. The "fake account, counterfeit card" scenario, where a transaction is performed using a counterfeit card that uses generated data that does not match any actual account (but often partially matches with fraudster). This is a fake card with an unauthorized user.

For situation one, the "friendly fraud" or "first-party fraud" scenario, the least cost avoider is the consumer. If it can be shown that the consumer did in fact perform the transaction, the consumer will bear the liability (assuming the consumer can be found and is solvent). In this scenario, there is no particular care that either the merchant or the issuer can take to avoid the fraud *ex-ante*. The transaction is indistinguishable from a legitimate purchase until the cardholder denies having made the transaction. At that point, the question is whether there is sufficient proof that the transaction was in fact properly authorized. Proof of authorization depends on the authorization method. If the merchant follows authorization protocols, then the issuer is the least cost avoider, as the issuer controls the authorization procedures. Accordingly, if the first-party fraud cannot be proven, the issuer

73. VISA DISPUTE PROCEDURES, *supra* note 68, at 100–07.

74. This Article does not address the various merchant-initiated fraud situations that can arise, including factoring for money laundering purposes.

bears the liability in the card-present environment. This means that liability rests on the least cost avoider.

For situation two, the "stolen card" scenario, if the consumer received the card, then the consumer is likely the least cost avoider, at least until the point that the card's theft is reported, at which point the issuer is the least cost avoider as the issuer can simply deactivate the card and deny any authorization requests.[75] Likewise, if the consumer did not receive the card because it was intercepted by a fraudster, then the issuer would be the least cost avoider as the issuer controls the card activation procedures.

The merchant is unlikely to be the least cost avoider for a stolen or intercepted card. The merchant might be able to recognize a card as stolen based on an obvious mismatch of the user and the name on the card—such as if Dolly Parton used Barack Obama's credit card—but card network rules do not expect merchants to catch obvious mismatches, and the merchant may generally not demand identification as a condition of accepting the card.[76]

Card network rules do generally require merchants to compare the signature on the charge slip with the specimen signature on the card,[77] but signature matching is an art, not a science, at least when practiced by store clerks, and is of little use in preventing fraud. The signature of a harried consumer, such as one in a grocery line attempting to soothe a bevy of bawling toddlers, is likely to vary significantly from a calmly written specimen. In a typical commercial context, the store clerk never examines the card in any way, not least because it is not an efficient use of the clerk's time. Even if a merchant's employees were diligent in examining signatures, the fraud reduction savings would likely be minimal. These savings would also be unlikely to offset the costs to the merchant from slower transaction speed at the register, namely the loss of sales because of greater transaction costs for customers due to increased wait times at the register or the cost of hiring more employees to work at the register. As

---

75. The major exception is the small minority of U.S. card transactions that are not authorized in real time (e.g., knucklebuster or telephone transactions). In those cases, the merchant may have parted with the merchandise before obtaining an authorization. When a merchant delivers without having obtained prior authorization, then the merchant is the least cost avoider.

76. MASTERCARD RULES, *supra* note 67, § 5.8.4, at 5-17; VISA INT'L REGULATIONS, *supra* note 67, at 468 (only requiring merchant review of additional identification where the signature panel is blank). The merchant may also require the cardholder's address or ZIP code for certain transactions. MASTERCARD RULES, *supra* note 67; VISA INT'L REGULATIONS, *supra* note 67, at 469. Discover requires merchants to examine two pieces of identification, one of which must be government issued for authorizing transactions on unsigned cards, but its rules are silent regarding examination of extrinsic identification for signed cards. *See* DISCOVER MERCHANT OPERATING REGULATIONS, *supra* note 67, § 3.1.2.1.

77. *See, e.g.*, MASTERCARD CHARGEBACK GUIDE, *supra* note 55, §§ 2.1.6.3.1–3.2; VISA INT'L REGULATIONS, *supra* note 67, at 463–64; DISCOVER MERCHANT OPERATING REGULATIONS, *supra* note 67, §§ 3.1.2–3.1.2.1.

with situation one, the ultimate least cost avoider in a stolen/lost card scenario is the issuer, and that is where liability rests.

In situation three, involving a fraudulently issued card, the issuer is the least cost avoider. There is no real consumer, and the merchant has even less ability to detect the fraud than with a stolen card, as the card information, including the signature, can be tailored to match that of the fraudster using the card. Again, the least cost avoider is liable.

In situation four, "real account, counterfeit card," it is not clear who is the least cost avoider. As the counterfeit card is made using real consumer data, data protection is the critical issue for preventing this type of fraud. The least cost avoider for data protection varies as data flows through the transaction process and is also retained for various purposes. But even with optimal data protection, there is still the possibility of "skimming"—the recording of card data from a magnetic stripe when the card is tendered to a merchant's employee (a particular problem in restaurants).[78] The skimmed data is then encoded onto a counterfeit card (or used in card-not-present transactions).

Thus for "real account, counterfeit card" the least cost avoider largely depends on how the fraudster obtained the real account information. Depending on how the information was obtained, the consumer, issuer, merchant or acquirer/processor could be at fault. Once the information is in circulation, however, the ability to prevent the counterfeiting largely depends on the issuer and the network and the security features they require for physical cards. The merchant is unlikely to detect the counterfeit. The merchant has no particular skill or ability to detect a counterfeit card beyond a blatantly poor forgery. This means the merchant has virtually no ability to stop the fraud. As the issuer controls the physical design of the card, and hence the ease of counterfeiting, the issuer is the least cost avoider, and yet again, the issuer is liable.

In situation five, with a counterfeit card using fake account information, the least cost avoider is likely the issuer. In this situation there is no actual consumer, and the merchant has little ability to detect the forgery. While the network and issuer have control over the physical characteristics of the card, which affect ease of counterfeiting, the issuer must authorize the transaction, and if the card does not match an existing account number, the issuer can easily deny the transaction. As with the other card-present scenarios, the issuer is the least cost avoider and is liable.

For card-present transactions, the least cost avoider may vary somewhat situationally, but it is typically the issuer. It makes sense to require the merchant to take basic anti-fraud steps and, if followed, place the loss on the issuer, who is then the least cost avoider. This is exactly what card

78. *See* Facciolo, *supra* note 8, at 629.

network rules mandate. Thus, the current arrangement of loss allocation for card-present rules seems largely sensible.

B. WHO IS THE LEAST COST AVOIDER? CARD-NOT-PRESENT TRANSACTIONS

Card-not-present transactions present a different story. CNP liability rules are a product of the historical development of payment card markets. When card networks first began, there were no CNP transactions. All transactions required physical presentment of the card, and the issuer bore the risk of unauthorized transactions (as explained above) as merchants were unwilling to assume fraud risk for a nascent technology over which they had little control.[79]

Merchants, however, wanted to be able to take cards for mail-order and telephone-order (MOTO) transactions, where no card would be presented physically.[80] Issuers were reluctant to assume fraud risk for these transactions, even if the expiry date was used as a password and merchandise was required to be sent to the cardholder's billing address.[81] Merchants concluded that the gains from these transactions outweighed the fraud risks, so they agreed to assume liability for unauthorized MOTO transactions[82] (certainly it was no riskier for them than shipping before a check was received and cleared).

The fraud liability rules made sense in their historical origins. Today, however, they are less sensible, as most CNP transactions are not MOTO, but Internet transactions. Historically, card fraud involved situations one through four (friendly fraud, stolen card, fraudulent issuance, counterfeit card using actual information), but not situation five (new account fraud). Fraudsters would obtain the card or card data of a real cardholder and would use it to purchase goods that would be shipped to the fraudster. Contemporary fraud involves both existing account fraud and new account fraud.[83]

The problem with CNP liability rules is that they do not account for changed circumstances. Now, as before, merchants have little ability to

---

79. Admittedly, until the 1970s, fraud prevention for card-present transactions was also quite difficult, as transactions were not authorized in real time. *See* ROSS J. ANDERSON, SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS 394–95 (Carol A. Long, ed., 2001); Steve Mott, *Perhaps It's Time to Mothball the Mighty Mag-Stripe*, PYMTS (2010), http://www.pymnts.com/perhaps-it-s-time-to-mothball-the-mighty-mag-stripe.

80. *See* ANDERSON, *supra* note 79, at 394.

81. *Id.* at 394.

82. *See* CYBERSOURCE, MANAGING RISK ON THE NET WHITE PAPER: WHAT INTERNET MERCHANTS NEED TO KNOW 2 (2000), *available at* http://www.cybersource.com/resources/collateral/pdf/ifs_wp111500.pdf.

83. Joseph Campana, Identity Theft: More than Account Fraud: What Everyone Should Know 1 (Apr. 2006) (unpublished manuscript), *available at* http://www.jcampana.com/JCampana Documents/IdentityTheftMoreThanAccountFraud.pdf.

prevent CNP fraud in any of these situations. The merchant's role in the transaction is limited to requiring whatever information the network and/or issuer require. The merchant has no ability to verify the information or the identity of the customer.[84] Moreover, CNP merchants face substantially higher interchange rates than card-present (CP) merchants in addition to a different set of fraud rules.[85]

Issuers' ability to prevent CNP fraud, however, has changed dramatically. Advances in card security arguably make CNP transactions safer than CP transactions.[86] In a CNP transaction, it is easy to require the cardholder to transmit not only the card account data and the Card Verification Value (CVV),[87] which is written on the back of the card and not included in the card number on the front or on the mag stripe, but also the billing address, billing telephone, or e-mail address information. If additional information beyond the card account data—the account number, the account holder's name, and the expiry data—is required, then a fraudster needs more than the physical card (which is easy to forge given that mag stripe technology is now over thirty years old[88]) or a copy of the face of the card to use the card successfully.

Accordingly, the issuer has the ability to prevent at least some CNP fraud. The issuer can first verify the information supplied to the merchant to ensure that it is a real account and that the card information matches the CVV code on the back of the card. Second, the issuer can verify the billing

---

84. *See* Mann, *Making Sense of Payments*, *supra* note 8, at 6771 (noting that in CNP settings, merchants lack a "credible mechanism for verifying the identity of the purported cardholder").

85. *See* DELL LETTER, *supra* note 3, at Appendix 1 (listing the "Differential Between Card Present and Card Not Present Visa Debit Interchange Fees"); Letter from Paul Misener, Vice President for Global Pub. Policy, Amazon.com, to Louise L. Roseman, Dir., Div. of Reserve Bank Operations and Payment Sys., Federal Reserve Board of Governors 14 (Nov. 20, 2010), *available at* http://www.federalreserve.gov/newsevents/files/amazon_comment_letter_20101120.pdf (showing that there is as much as a 98 basis point and two cents difference in CNP and CP interchange rates); *see also* Letter from Joshua R. Floum, Exec. Vice President, General Counsel and Secretary, Visa U.S.A., Inc., to Louise L Roseman, Dir., Div. of Reserve Bank Operations and Payment Sys., Federal Reserve Board of Governors 13 (Nov. 8, 2010), *available at* http://www.federalreserve.gov/newsevents/files/visa_comment_letter20101118.pdf (noting that interchange rates reflect fraud risks).

86. *See generally* VISA, GLOBAL VISA CARD-NOT-PRESENT MERCHANT GUIDE TO GREATER FRAUD CONTROL: PROTECT YOUR BUSINESS AND YOUR CUSTOMERS WITH VISA'S LAYERS OF SECURITY, *available at* http://usa.visa.com/download/merchants/global-visa-card-not-present-merchant-guide-to-greater-fraud-control.pdf.

87. This code is variously called the Card Security Code (CSC), Card Verification Value (CVV or CV2 or CVV2), Card Verification Value Code (CVVC), Card Verification Code (CVC), Verification Code (V-Code or V Code), or Card Code Verification (CCV). The two included in some abbreviations is to distinguish it from the code on the front on the card and mag stripe (the card number). *See* Kimberly Kiefer Peretti, *Data Breaches: What the Underground World of "Carding" Reveals*, SANTA CLARA COMP. & HIGH TECH. L.J. 375, 387 n. 66 (2009); *see also Card Security Code (CSC) and Card Verification Value (CVV)*, BOOTSTRAP, http://mediakey.dk/~cc/card-security-code-csc-and-card-verification-value-cvv (last visited Oct. 19, 2010).

88. *See* Mott, *supra* note 79.

address or other borrower information. Third, the issuer can use statistical fraud prevention tools called neural networks that can identify anomalies in spending behavior by analyzing transactions in relation to the cardholder's transaction history, looking for outliers in geography, merchant type, and transaction amount. The speed of these networks allows issuers to prevent suspicious transactions at the authorization stage.

Thus, if an 18-year old Peoria resident's card was used at 5PM CDT to make a purchase at a fast food restaurant in Peoria, and then used at 5:15PM CDT to purchase a $2,000 dinner in Paris, there is likely a fraud occurring. The issuer can deny the questionable transaction and freeze the account until and unless the real cardholder contacts the issuer to unlock the account by providing some additional verification information.[89] Critically, only the issuer has the ability to examine data from multiple transactions to observe transaction patterns; merchants only observe one-off transactions.

Issuers' ability to prevent unauthorized CNP transactions has advanced by leaps and bounds since the 1970s, when MOTO transactions began.[90] Moreover, issuers no longer need to be induced to authorize CNP transactions; e-commerce is so well established that issuers cannot and would not abandon the market if they were to bear liability for unauthorized transactions.

The efficiency of CNP liability rules is suspect in light of changes in the marketplace. Originally, it made sense for merchants to bear the risk of fraud on CNP transactions because there was no effective avoidance and because merchants gained the greatest benefit from the transactions. Now issuers are the clear least cost avoider. Accordingly, placing the liability on issuers would be the efficient outcome; indeed, it would likely encourage greater security efforts, such as the use of two-factor identification methods that rely on factors other than CVV and billing address, such as a randomly generated PINs, which would be known only to the cardholder, absent cardholder carelessness.[91]

C. MAKING SENSE OF THE LIABILITY RULES

Payment card network rules for allocating liability for unauthorized transactions seem well-designed for card-present transactions, but are

89. To be sure, the issuer's ability to prevent fraud is far from perfect. Small ticket, local transactions are unlikely to get noticed. But compared to the merchant, the issuer has much greater ability to avoid the fraud. Yet, liability for CNP transactions is not on the issuer.

90. ANDERSON, *supra* note 79, at 394.

91. To be sure, we might ask whether their current situation is Kaldor-Hicks efficient. Why don't merchants simply pay issuers for greater security measures up to the point where there would be no marginal benefit? The answer is because of a coordination problem due to high transactions—there are millions of merchants and thousands of issuers that must be coordinated—and because of a free-riding problem. The benefits of improved issuer fraud prevention are shared by all merchants. If any merchant paid for better security, it would have to share the benefits with free-riders. Better, a merchant would calculate, to free-ride, than to be freely ridden.

unlikely to be optimal in a CNP setting. Figure 2 summarizes the variations between actual rules and the likely optimal rules, assuming that all authorization procedures are properly followed by the merchant.

Figure 2. Actual and Likely Optimal Fraud Allocation Rules

	EXISTING ACCOUNT FRAUD		NEW ACCOUNT FRAUD	
	ACTUAL RULE	OPTIMAL RULE	ACTUAL RULE	OPTIMAL RULE
CARD PRESENT	ISSUER	ISSUER	ISSUER	ISSUER
CARD NOT PRESENT	MERCHANT	ISSUER	MERCHANT	ISSUER

Why would the United States have suboptimal liability rules for payment card networks? Part of the answer is historical. As Part II.B. explained, for CNP transactions, rules that made sense in their original context have ossified and become outmoded by changes in technology.

The history of the payment card networks themselves explains this ossification. Until 2005–2006, MasterCard and Visa, the largest payment card networks, were mutual organizations dominated by their large issuer banks.[92] The large issuer banks had little incentive to change the CNP liability rules. Under the rules, issuers incur fraud losses that are only a fraction of merchants'.[93] Thus in 2009, issuers incurred $0.95 billion in total (CP and CNP) fraud losses.[94] In contrast, one study puts merchants' total fraud losses at over $100 billion.[95] While issuers are the least cost avoiders, they do not bear most of the costs of fraud. Therefore, they have little incentive to engage in aggressive anti-fraud efforts.[96] For example, networks and issuers have persisted in using mag stripe cards with account numbers embossed on the front.[97] These cards are extremely vulnerable to

92. Levitin, *Economic Costs*, *supra* note 19, at 1327–28.

93. LEXISNEXIS FRAUD STUDY, *supra* note 1, at 23.

94. Kate Fitzgerald, *supra* note 1, at 17.

95. LEXISNEXIS FRAUD STUDY, *supra* note 1, at 23.

96. In theory, in the credit card space, the other two networks, American Express and Discover, could have tried competitive differentiation based on different CNP fraud rules. However, these networks had little to gain from such differentiation. At best, it would increase their merchant acceptance rates, but it would not necessarily garner them more transactions, as merchants do not choose which card network a payment will be on. Moreover, these networks are also their own primary issuers (and were their sole issuers before 2005), so the competitive benefits from signing up more merchants would have to be weighed against the network-issuer incurring greater fraud losses. The calculus, apparently, weighed in favor of keeping the losses on merchants. For debit cards, CNP transactions have never been a critical issue because there are very few CNP debit transactions. MOTO and Internet debit transactions are rare.

97. *See* Mott, *supra* note 79.

skimming, to use when they are stolen, and to having account numbers simply copied down and then used in CNP transactions.[98] Simple steps such as adopting Chip & PIN technology (discussed in more detail in the next section) would frustrate skimming and theft, while card numbers need not be displayed on the card.[99]

Anti-fraud efforts must be implemented by issuers, but the role of setting standards falls to the network association itself. The problem is that the network associations compete with each other for issuer membership. The networks make most of their revenue from per transaction fees.[100] This means that they want to increase volume on their cards, which in turn means that they need to have more cards in circulation. In order to increase the number of cards, networks need to have more and larger issuers in their stables. Networks thus compete for issuers.

If a network required greater anti-fraud measures from issuers, it would impose additional costs on issuers and therefore make itself less attractive to them. The full cost of anti-fraud would be borne by the issuer, but the benefits would accrue primarily to the merchant, and issuers have little interest in subsidizing merchants for the overall good of the network. Mandating additional anti-fraud measures can cost a network market share, while bringing the network itself no tangible benefit.

D. INTERNATIONAL VARIATION IN LIABILITY RULES AND FRAUD ARBITRAGE

1. International Variation

There is significant international variation in payment card fraud liability allocation rules.[101] The international variation suggests that private ordering does not always produce optimal results. It is possible that

---

98. *Id.*

99. The short-lived Revolution Card (purchased by Amex in 2010) did not have an account number visible on the front and required a PIN for all transactions. *See* What is RevolutionCard?, REVOLUTIONCARD, http://www.revolutioncard.com/what-is-revolutioncard.aspx (last visited Oct. 9, 2010)

> RevolutionCards don't display your name, signature or other personally identifying information on the card, offering you unparalleled security. So, even if you lose your card, no one knows it's yours, and if they do find out, they can not use it without your PIN. RevolutionCards are PIN-based, and members can create their own unique 4-digit Card Authorization Code (CAC) that is entered as a PIN into the PIN-pads at merchants locations, and can be used for online shopping and phone-orders. Cardholders can also generate random One Time CAC numbers, so they never need to give out their primary CAC/PIN when they are using the card for online purchases, phone or other card-not-present transactions.

Id.

100. *See* DeGennaro, *supra* note 45, at 28.

101. *See* MASTERCARD RULES, *supra* note 67, §§ 3.9.1, at 11-1, 3.9.1(3), at 14-2 (corresponding rules in the Canada and the South Asia, Middle East, and Africa regions).

different orderings are optimal in different countries, perhaps reflecting variations in market penetration by payment cards. Yet there are variations, even among very similarly developed economies with similar payment card market penetration and usage patterns.

Such variation is evidence that private ordering might not always result in optimal liability rules. But it does not tell us which, if any, of the private orderings is optimal. There is reason to believe, however, that the private ordering in the United States is suboptimal compared with systems around the world. Financial institutions in virtually every developed economy outside of the United States have adopted integrated circuit (IC), or chip cards, as their standard.[102] Chip cards contain a microchip in the card.[103] The microchip is, like any microchip, multifunctional,[104] but among its chief purposes is that it allows a card reader that operates on the same standard, known as EMV (short for EuroPay-MasterCard-Visa), to verify the authenticity of the card. The chip is thus an anti-counterfeiting device. Australia, Canada, Cambodia, China, Hong Kong, Indonesia, Japan, Korea, Malaysia, New Zealand, Singapore, South Africa, Taiwan, United Arab Emirates, and virtually all of Europe have adopted EMV technology.[105] Unlike the traditional mag stripe card, a chip card is quite difficult to counterfeit.

The chip technology itself is only a protection against counterfeiting physical cards, including duplication of actual cards. The chip does not prevent unauthorized transactions if a card is stolen.[106] In some countries and regions, such as Australia, Canada, and Europe, financial institutions have gone further to require Chip & PIN technology, where the IC card can only be used with a PIN.[107] Thus in Europe, all new, upgraded, or replaced point-of-sale chip terminals must have a PIN pad.[108]

The PIN provides two-factor identification (the first factor being possession of the card) where one factor is separate from the card (unlike CVV), and helps ensure not only that the card is genuine, but that it is being used by its authorized user.[109] Thus, the Oliver Wyman Group reports that in 2008 fraud loss rates on signature debit cards in the United States were

---

102. *See* John Hill & Victoria Conroy, *EMV: The Story So Far*, CARDS INT'L, Apr. 2009, http://www.vrl-financial-news.com/asia-pacific/banking--payments-asia/issues/bpa-2009/bpa-2009/emv-the-story-so-far.aspx; Thad Rueter, *U.S. Stays on Sidelines As Other Nations Make EMV Game Plans*, CARDS & PAYMENTS, Nov. 2009, at 14, 16.

103. *See* Mott, *supra* note 79 ("Payment Cards 'Smart'").

104. *Id.* ("Is Contactless the New Hope?").

105. Hill & Conroy, *supra* note 102; Rueter, *supra* note 102.

106. *See* Hill & Conroy, *supra* note 102.

107. MASTERCARD RULES, *supra* note 67, § 12-3.9.1(3), at 12-15.

108. *Id.* (discussing PIN Entry Device Mandate for the European Region). In Europe, issuers are also forbidden from authorizing CNP transactions unless there is CVC2 verification. *Id.* § 3.9.2, at 12-15 ("CVC Processing for Card-Not-Present Transactions").

109. Claes Bell, *Are Chip and PIN Credit Cards Coming?*, BANKRATE.COM (Feb. 2, 2010), http://www.bankrate.com/finance/credit-cards/are-chip-and-pin-credit-cards-coming-1.aspx.

7.5 basis points, whereas PIN debit fraud loss rates were only one basis point.[110] Although Chip & PIN is not a failsafe technology, it is a far stronger safety measure than anything on the American market.[111]

In the United States, only two cards have been rolled out with a chip: the American Express Blue Card (Blue), first introduced in 1999,[112] and the United Nations Federal Credit Union (UNFCU) Visa card, introduced in 2010.[113] Blue is American Express's non-exclusive, mass-market card.[114] Blue enables Amex to charge its premium merchant discount fee rates for non-premium cardholders. While Amex equipped Blue cards with a chip, the chip is useless as a security measure as almost no American merchants have chip readers.[115] Instead of serving as a security measure, the chip is used for storing information about rewards programs.

The UNFCU Visa card, in contrast, does use Chip & PIN for security reasons.[116] UNFCU moved to Chip & PIN technology both because it experienced particularly high fraud rates and because many of its members use their cards outside of the United States in countries where Chip & PIN is the norm and plain mag stripe cards are sometimes refused.[117] In the United States, though, the UNFCU Visa card operates just as a regular mag stripe card, and it gains no security benefits from its Chip & PIN capability due to the lack of Chip & PIN enabled point-of-sale terminals.[118]

Card network rules provide that use of Chip and Chip & PIN technologies has been coupled with a shift in liability for card-present transactions. Under the liability shift, merchants become, by default, liable for all unauthorized card-present transactions.[119] But, if the transaction used a Chip reader, then the merchant will not be liable for losses from counterfeit cards; instead liability will shift back to the issuer.[120] Similarly,

---

110. Stephanie Bell, *Study: Debit Fraud Rates Rose Sharply Last Year*, AM. BANKER, May 21, 2010, at 6.

111. Stephen J. Murdoch et al., *EMV PIN Verification "Wedge" Vulnerability*, UNIV. OF CAMBRIDGE, http://www.cl.cam.ac.uk/research/security/banking/nopin (last visited Dec. 30, 2010); *see also* Ross Anderson et al., Chip and Spin (May 2005) (unpublished manuscript), *available at* http://chipandspin.co.uk/spin.pdf; Saar Drimer et al., Optimised to Fail: Card Readers for Online Banking 8–12 (Feb. 26–29, 2009) (unpublished manuscript), *available at* http://www.cl.cam.ac.uk/~sjm217/papers/fc09optimised.pdf (last visited Oct. 9, 2010).

112. Jennifer Kingson*, A Credit Card Loses Its High-Tech Cred,* N.Y. TIMES BITS BLOG (Dec. 5, 2008*,* 11:30 AM), http://bits.blogs.nytimes.com/2008/12/05/a-credit-card-loses-its-high-tech-cred*.*

113. David Morrison, *United Nations FCU Becomes First Chip and PIN Card Issuer in the U.S.*, CREDIT UNION TIMES (May 26, 2010), http://www.cutimes.com/Issues/2010/May-26-2010/Pages/United-Nations-FCU-Becomes-First-Chip-and-PIN-Card-Issuer-in-the-US.aspx.

114. Query, is "Blue" short for blue collar?

115. Morrison, *supra* note 113.

116. *Id.*

117. *Id.*

118. *See id.*

119. MASTERCARD CHARGEBACK GUIDE, *supra* note 55, § 2.8.2.

120. *Id.*

if the transaction is with a Chip & PIN card and is properly used with an EMV reader, then liability for unauthorized transactions shifts back to the issuer.[121]

These liability-shifting rules are consciously designed to encourage merchant adoption of EMV readers. Some card networks have also encouraged this shift by imposing an "incentive interchange rate"—interchange penalties and rewards. In some regions, MasterCard offers a ten basis point reduction in interchange for Chip & PIN transactions, and imposes a ten basis point penalty for non-Chip & PIN card-present transactions.[122]

At least for MasterCard, the decision of whether to implement a Chip liability shift is left up to the financial institution members of the network—not the merchants who are also affected. MasterCard permits a Chip liability shift program in any country or region in which MasterCard member financial institutions representing "75 percent of the currency volume of both acquiring and issuing transactions" approve.[123] Thus, Europe has had a Chip liability shift since January 1, 2005, Brazil since March 1, 2008, Columbia since October 1, 2008, and Venezuela since July 1, 2009. In Canada, Africa, Asia, and the Middle East the shift took effect on October 15, 2010.[124] Intraregionally, Europe, Latin America, and the Caribbean have had Chip liability shifts since 2005.[125]

---

121. *Id.*; VISA DISPUTE PROCEDURES, *supra* note 68, at 102 (noting that a chargeback is invalid "if the Device is EMV PIN-Compliant and the Transaction was correctly processed to completion in accordance with EMV and VIS using the Chip Card data").

> For purposes of these Rules, "EMV-compliant" means in compliance with the EMV standards then in effect.
>
> 1. **Chip Liability Shift.** The liability for intraregional counterfeit fraudulent Transactions in which one Regional Member (either the Issuer or the Acquirer) is not yet EMV-compliant is borne by the non–EMV-compliant Regional Member.
>
> 2. **Chip/PIN Liability Shift.** The liability for intraregional lost, stolen, and never received fraudulent Transactions in which one Regional Member (either the Issuer or the Acquirer) is not yet able to support chip/PIN Transactions is borne by the non-chip/PIN-compliant Regional Member.

MASTERCARD RULES, *supra* note 67, § 3.9.1, at 12-14.

122. MASTERCARD RULES, *supra* note 67, § 3.9.1(2), at 10-2 (applicable to the Asia & Pacific Region); *id.* § 3.9.1(4), at 10-3 (applicable to the Latin America and Caribbean Region); *id.* § 3.9.1(2), at 14-2 (applicable to the South Asia, Middle East and Africa Regions). This implies that MasterCard believes that in these regions, the total costs of fraud borne by merchants plus the cost of investing in Chip & PIN readers is less than twenty basis points.

123. MASTERCARD CHARGEBACK GUIDE, *supra* note 55, §2.8.2.4.1.1, at 2-54.

124. MASTERCARD RULES, *supra* note 67, § 3.9.1, at 11-1 (corresponding to the Canada Region); *id.* § 3.9.1(3), at 14-2, 14-3 (corresponding to the South Asia, Middle East, and Africa, regions).

125. MASTERCARD WORLDWIDE, CIRRUS WORLDWIDE OPERATING RULES, § 11.1.1 (Sept. 15, 2010). As MasterCard notes:

The absence of Chip & PIN technology in the United States bears comment. It is widely recognized that Chip & PIN technology significantly reduces fraud losses.[126] In the UK, losses on fraud in face-to-face (card-present) transactions fell from £135.9 in 2005 to £72.1M in 2009.[127] So why hasn't Chip & PIN been adopted in the United States?

An initial answer may be that it is simply not efficient from a system-wide perspective. While readily comparable international fraud loss rate data is not available, the United States was historically reputed to have relatively low fraud loss rates, in part due to low cost telecommunications that made real-time authorization possible.[128] Moreover, total fraud losses on payment cards are noticeably lower than on competing payment methods, such as checks.[129] If payment card fraud costs are sufficiently low, then there may simply not be an economic case for adopting Chip & PIN. On the other hand, a recent study estimates that U.S. payment card fraud losses rates are higher in the U.S. than in Australia, France, Spain, and the UK.[130]

It is not clear, however, whether Chip & PIN would be an inefficient overinvestment in fraud prevention technology. Another explanation is that Chip & PIN implementation is actually an efficient investment, but it is stymied by the organization of and conflicts of interest in payment card networks, which fail to properly incentivize parties to take optimal care in preventing fraud.

> EMV chip technology can provide a more secure alternative to non-chip technology for reducing fraudulent Transactions. Therefore, certain countries and Regions have decided to migrate to the EMV chip platform.
>
> Many of these same countries and Regions have instituted a chip liability shift program for domestic and intraregional Transactions to protect Members that have made the early investment in EMV chip.
>
> . . .
>
> Chip liability shift means that when a counterfeit fraud Transaction occurs in a country or Region that has migrated to the Chip platform the liability for the Transactions will shift to the non-chip-compliant party.

Id.

126. *See* Rueter, *supra* note 102.

127. *Facts and Figures*, UK CARDS ASS'N, http://www.theukcardsassociation.org.uk/view_point_and_publications/facts_and_figures (last visited Oct. 9, 2010).

128. *See* Mann, *Credit Cards and Debit Cards*, *supra* note 8, at 1069–70, 1090–91 (noting the role of telecommunications costs in determining payment card fraud resistance).

129. Chris Costanzo, *Combating Fraud*, BANK DIRECTOR MAG., Q1 2007, http://www.bankdirector.com/issues/articles.pl?article_id=11865. It is unclear if fraud loss rates are lower for checks currently; historically they were. *See* William Roberds, *The Impact of Fraud on New Methods of Retail Payment*, FED. RESERVE BANK OF ATLANTA ECON. REV., 2Q 1998, at 42, 45, *available at* http://www.frbatlanta.org/filelegacydocs/Roberd.pdf (noting a 2 basis point loss rate for checks compared with 18 basis point loss for credit cards in 1995).

130. Sullivan, *supra* note 1, at 110, 112–14.

Merchants have no ability to adopt Chip & PIN; they are not part of card networks and cannot change card network rules. Moreover, there is little reason for them to invest in Chip & PIN enabled point-of-sale terminals unless issuers are issuing Chip & PIN Cards. As acquirers pass fraud costs through to merchants, they have little interest in the matter. Only issuers have a direct interest and are part of card networks. Issuers, however, do not want to incur the cost of having to reissue cards to make them Chip & PIN capable. The counterfeiting losses in the United States do not justify the reissuance expense of issuers, and for debit cards, issuers do not want to see transactions shift from signature debit cards (which have higher interchange rates) to PIN debit cards.[131] Card network organization structure and economics frustrate the adoption of the best technology for fraud prevention.

2. Fraud Arbitrage

International variation in fraud liability and security rules creates opportunities for fraud arbitrage, thereby undermining security systems. Fraudsters, often highly organized, use cards from more secure locations in less secure ones.[132]

In particular, the lack of Chip & PIN protection in the United States undermines Chip & PIN systems abroad.[133] For example, Canada has adopted Chip & PIN technology, but Canadian credit cards can be used to pay in the United States.[134] When a Canadian card is used in the United States, it is used without a Chip & PIN because almost no American merchants have Chip & PIN capable readers.[135] Canadian fraudsters know that they merely have to use stolen Canadian card numbers in the United States. Furthermore, Canadian consumers and merchants might be less vigilant about protecting their physical cards because of the lulling effect of

---

131. Kate Fitzgerald, *Calculating the Cost: Debit Fees Could be Cut by $5B*, AM. BANKER, June 28, 2010, at 1 (noting higher interchange rates on signature debit cards than on PIN debit cards). This shift may happen regardless because of the Durbin Interchange Amendment. Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, Pub. L. No. 111-203, § 1075, 124 Stat. 1376, 2068–74 (2010).

132. *See* Rueter, *supra* note 105, at 14, 17.

133. *US at Risk of Becoming "A Centre For Card Fraud*", CARDS INT'L, AUG. 2010, http://www.vrl-financial-news.com/cards--payments/cards-international/issues/ci-2010/ci-445-446/us-at-risk-of-becoming-a-centr.aspx; Ian Kerr, *Challenges in Migrating to EMV*, ATM MEDIA RESOURCE CENTRE (Mar. 11, 2010, 3:19 PM), http://www.atmindustryinfo.com/2010/03/challenges-in-migrating-to-emv.html (fraud migrated from EMV adopters in Singapore and Malaysia to non-EMV Thailand); Rueter, *supra* note 102, at 14 (discussing shift of fraud from EMV-enabled UK to non-EMV countries and from Canada to US with Canadian adoption of Chip & PIN security).

134. *See* Rueter, *supra* note 102.

135. For example, Wal-Mart's POS terminals are Chip & PIN capable, but Wal-Mart does not actually use the terminals for Chip & PIN transactions when presented with a Chip & PIN card. *See* Kate Fitzgerald, *Wal-Mart Claims Issuers Block Progress of EMV Cards in U.S.*, AM. BANKER, May 24, 2010, at 7.

two-factor Chip & PIN identification; Canadian consumers believe that the card by itself is useless without the PIN—and it is—but not when the card is used south of the border.

Another variation of this international fraud arbitrage problem is the use of European cards in the United States. The Chip & PIN arbitrage also exists between Europe and the United States, but there is another variation in security as well.[136] In the United States, real time authorization is the key line of fraud prevention.[137] Because of historically high telecommunications costs, however, Europe does not use real time authorization systems.[138] Instead, European anti-fraud efforts were channeled into better security features in the cards and the terminals—Chip & PIN.[139] When European cards are used in the United States, the worst of both worlds exists. The superior card and terminal security features are not functional, and there is no real time authorization.

III. REGULATORY INTERVENTIONS

A. THE COORDINATION PROBLEM IN PAYMENT CARD NETWORKS

The problems of international fraud arbitrage speak to the core coordination issue in payment systems. Payment systems are the backbone of the economy; they are the infrastructure of commerce. Payment systems allow commerce to move beyond barter by creating a common liquid medium for exchanging value. Liquidity requires standardization. Standardization is the lubricant of exchange, and every successful payment medium has been standardized to a greater or lesser degree: wampum, cell phone minutes, gold, or electronic payment commands.

Standardization includes standardized security measures. The security measures (or lack thereof) of individual participants in a payment system may have positive or negative externalities on other system participants. A participant's strong security measures can help deter fraud generally and catch fraudsters as well as frustrate attempts to obtain data that can be used to defraud other system participants. Similarly, lax security measures (such as poor data security) can result in fraud losses at other system participants. Payment system participants do not internalize these costs or benefits, however, so left to their own devices, they may not achieve the optimal level of security.[140] Mandatory coordination among system participants is

136. *See* Sullivan, *supra* note 1, at 115 (noting that with Chip & PIN adoption in the UK, UK counterfeit card fraud is now mainly done on transactions in the U.S. because of lack of Chip & PIN adoption in U.S.).

137. Rueter, *supra* note 102, at 16.

138. *See* Mott, *supra* note 79; *see also supra* note 128 and accompanying text.

139. *See* Kerr, *supra* note 133.

140. *See* Sullivan, *supra* note 1, at 118.

critical, then, for optimizing security measures and promoting positive externalities.

Accordingly, participation in various payment systems is dependent upon abiding by system standards. These standards are sometimes indirect and mandatory by public law, such as bank safety and soundness requirements like Know Your Customer rules. Other times, they are private law that operate through contract, such as membership in a payment card network or a check clearinghouse or automated clearinghouse.

Standardization requires a standard setting process. One of the major roles of payment card networks is standard setting. For multi-institution networks, this is a tremendous coordination task. International fraud arbitrage shows that in a global economy, international standards are needed for data security.[141] It is insufficient for standards to be nationally based. If electronic payments are to be global currency, they need uniform security standards.

Setting standards in payment card networks involves coordinating between multiple parties.[142] For multi-issuer networks, such as MasterCard, Visa, and all the PIN debit networks, it is necessary to coordinate between numerous issuers and acquirers. This often involves the network acting unilaterally; the transaction costs of individual issuer-acquirer negotiations for networks that can involve 16,000[143] financial institutions are simply too great. Similarly, merchants' dealings with the networks via their acquirer banks cannot readily be individually negotiated; there would need to be too many negotiations. Coasean bargaining is not possible given the transaction costs in multi-party networks.

Given the impracticality of Coasean bargaining with payment systems, how can we hope to optimize outcomes? The answer lies in highlighting both cooperative and competitive features of payment card networks. Payment card networks represent an unusual confluence of competition and cooperation, or as David Evans and Richard Schmalensee have termed it, "co-opetition."[144] Improving fraud loss liability allocations involves two seemingly contradictory moves, each of which playing to a different aspect of co-opetition. First, coordination problems can be smoothed over by encouraging greater security coordination between card networks (and their participants). Second, antitrust enforcement on the long-simmering interchange issue—which has been only partially resolved by the Durbin

---

141. *See supra* Part II.D.2.

142. *See supra* Part I.A.

143. VISA INC., CORPORATE OVERVIEW 2, *available at* http://phx.corporate-ir.net/External.File?item=UGFyZW50SUQ9NDYxMzZ8Q2hpbGRJRD0tMXxUeXBlPTM=&t=1.

144. DAVID S. EVANS & RICHARD SCHMALENSEE, PAYING WITH PLASTIC: THE DIGITAL REVOLUTION IN BUYING AND BORROWING 7 (2nd ed. 2005).

Interchange Amendment[145] and the antitrust litigation brought by the Department of Justice and seven states against MasterCard, Visa, and American Express[146]—will ensure that there is true price competition in the payment card market between networks and merchants. As fraud liability is a component of price, enabling price competition will help achieve a result closer to that of Coasean bargaining. In the presence of overwhelming transaction costs, strong competition can substitute for Coasean bargaining.

B. ENCOURAGE BETTER GOVERNANCE FOR SECURITY STANDARD COORDINATION

Payment card security measures are largely undertaken at the network level;[147] the network mandates particular practices, and issuers and acquirers must comply.[148] Despite most security measures being mandated on the network level, networks do not compete on security measures for end-users. Merchants, who bear the bulk of fraud losses, are indifferent to variations in networks' security measures. Most merchants accept cards from multiple networks, and to the extent that they do not accept particular networks' cards, it is usually because of interchange fees, not security rule variations. Merchants typically get bundled acquiring (or at least processing) services; the acquirer or processor will handle all of the merchant's payment card transactions using the same interface.[149] Thus, from the merchant's perspective there is no difference between card networks except pricing; security distinctions are invisible to the merchants.

Similarly, consumers are utterly indifferent to network-level security mandates. The federal consumer liability limitation for unauthorized payment card transactions and the networks' zero liability policies for unauthorized transactions reduce consumers' incentive to care about card security measures.[150] Consumers have no contractual privity with the network and see no difference in card functionality between networks. A MasterCard and a Visa credit card are completely interchangeable from a consumer's perspective, and issuers will sometimes switch consumer's accounts among networks. Likewise, the same debit card is often an access device for multiple debit card networks: Accel, Cirrus, Interlink, NYCE,

145. *See* Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, Pub. L. No. 111-203, § 1075, 124 Stat. 1376, 2068–74 (2010).

146. *See* Complaint, United States v. Am. Exp., Co., No. 1:10-cv-04496 (E.D.N.Y., Oct. 4, 2010) (alleging violations of Section 1 of the Sherman Antitrust Act based on various card network merchant restraint rules); [Proposed] Final Judgment, United States v. Am. Exp., Co., No. 1:10-cv-04496 (E.D.N.Y., Oct. 4, 2010).

147. Douglass, *supra* note 9, at 45.

148. *See id.*; Ballen & Fox, *supra* note 9, at 940–41.

149. *See* EVANS & SCHMALENSEE, *supra* note 144, at 6–7.

150. Note, however, that not all debit card networks have zero liability policies. Given the low rate of PIN debit fraud and the existing Regulation E limitations on consumer liability, such a zero liability policy would not mean much to consumers.

Plus, Pulse, Star, etc.[151] Consumers never select what networks will have preferred routing flags on their debit cards; that choice is left to their banks.

While most security features are mandated by the networks, there is variation among issuers in security features and practices. In particular, issuers' fraud detection relies heavily on neural networks, but individual issuers have their own neural network designs. Consumers have little reason to care about variations in issuer anti-fraud measures, as they are almost never themselves liable, and, perhaps more importantly, they cannot gauge the value of anti-fraud technologies. There is no way for a consumer to know whether a particular issuer's technology is better than another's. Fraud protection is not like a burglar alarm. There are a limited number of ways into a dwelling, and a consumer can, in theory, test an alarm system against simulated burglary. The same cannot be done for card fraud.

Because payment card end-users are indifferent to variations in networks' anti-fraud measures, there is little reason to foster competition among networks on security measures. Bundled merchant services and consumer indifference mean that networks have little incentive to compete in terms of security measures. Indeed, because the costs of security measures are borne by issuers, while most of the benefits accrue to merchants, issuers are resistant to greater security measures. A network that unilaterally imposes more demanding and costly security measures risks losing issuer business to other networks.

Given that the market is structured against competition for heightened security measures, how can we encourage greater security measures in payment card networks? One way is to encourage coordination among networks. If networks could coordinate security measures, they could adopt them uniformly, thereby eliminating market pressure from issuers for lower security measures. Security measures are an area where we might actually want some type of standard setting. (And, to the extent that we view security standards as a form of price, price-fixing!)

Network coordination should be guided by the principle of locating what method would benefit the overall payment card industry—that is, a net social welfare gain—rather than what would increase the size of any particular network—that is, a gain to any particular competitor. Coordination on security measures would essentially liberate the networks to engage in more effective allocation of that portion of price among network participants.

The card networks have already devised a corporatist form of coordination using the Payment Card Industry Security Standards

---

151. *See, e.g.*, FUMIKO HAYASHI, RICHARD SULLIVAN & STUART E. WEINER, PAYMENT SYS. RESEARCH DEP'T, FED. RES. BANK OF KANSAS CITY, A GUIDE TO THE ATM AND DEBIT CARD INDUSTRY 20 (2003), *available at* http://www.kansascityfed.org/publicat/PSR/BksJournArticles/ATMpaper.pdf.

Council.[152] PCI SSC is a nominally independent organization created by the card networks to promulgate non-binding data security standards for payment cards.[153] PCI SSC is owned by the five major credit card networks (American Express, Discover Financial Services, JCB International (Japan Commerce Bank), MasterCard WorldWide, and Visa, Inc.).[154] Each network appoints an officer to the PSC SSC executive committee and management committee. PCI SSC has 612 "participating organizations," including financial institutions and intermediaries of various sorts, trade associations, and merchants ranging from Wal-Mart to the University of Notre Dame.[155] Participating organizations get to nominate and vote for the PCI SSC's twenty-member Board of Advisors (which currently only has four representatives from entities classified as "merchants") and to review proposed PCI standards and revisions thereto, including the Payments Card Industry Data Security Standards (PCI DSS), before they are made public. Neither participating organization nor the Board of Advisors has any formal ability to determine the standards.[156] While PCI SSC cannot itself enforce the PCI DSS because it does not have a contractual relationship with card network participants, all of the networks incorporate the PCI DSS in their rules, and require network participants to be PCI DSS compliant.[157]

To date, the operation of the PCI SSC has been controversial.[158] Networks and issuers play a leading role in PCI SSC, and merchant groups complain that PCI DSS is geared toward advancing issuers' interests.[159] In particular, merchant groups object to PCI SSC data retention requirements, which issuers want because of chargeback issues.[160] PCI SSC requires

---

152. Epstein & Brown, *supra* note 9, at 214–15.

153. *Id.* at 215.

154. About the PCI Security Standards Council, https://www.pcisecuritystandards.org/organization_info/index.php (last viewed Dec. 30, 2010).

155. Participating Organizations, PCI SECURITY STANDARDS COUNCIL, https://www.pcisecuritystandards.org/get_involved/member_list.php?category=&region= (last viewed Dec. 30, 2010).

156. Participating Organization Rights, Obligations and Rules of Participation, PCI SECURITY STANDARDS COUNCIL, https://www.pcisecuritystandards.org/get_involved/rights_responsibilities.php (last visited Dec. 30, 2010).

157. *See* Epstein & Brown, *supra* note 9, at 214–215; *see also* DISCOVER MERCHANT OPERATING REGULATIONS, *supra* note 67, at ix; AMERICAN EXPRESS MERCHANT REFERENCE GUIDE—U.S. (Apr. 2010), *supra* note 67, § 8.3; VISA INT'L REGULATIONS, *supra* note 67, at 684. Non-compliant merchants face higher, penalty interchange rates. The particular form of this coordination is shaped by antitrust concerns. Epstein & Brown, *supra* note 9, at 215.

158. *See* Sullivan, *supra* note 1, at 120.

159. *Id.*

160. *See* David Taylor, *Moving Beyond PCI*, CARDS & PAYMENTS, May 2009, at 40 (noting that "tokenization, seeks to remove card data from the retail environment as soon as possible and substitute account numbers with 'fake,' or one-time, numbers that have no intrinsic market value"); Avivah Litan, *Where to Begin for End-to-End Encryption Systems*, AM. BANKER, Sept. 15, 2009, at 15 (arguing that "[p]ayments companies will also need to change some business processes, so that merchants are not required to hold on to card data for business purposes, such as resolving chargebacks, or preauthorization and presettlement processes").

merchants to retain certain transaction data.[161] While the data is supposed to be encrypted and otherwise protected, merchants object that the mere presence of large volumes of transaction data make them tempting targets for fraudsters.[162]

Moreover, the effectiveness of the PCI DSS is unclear. Heartland Payment Systems, Inc., a major card processor, was subjected to hacking from December 2007 until October 2008, during which time 130 million records were stolen.[163] Heartland was certified as PCI DSS compliant in April 2008.[164] Visa disputes Heartland's PCI DSS compliance.[165] In 2009, a data security breach occurred at Network Solutions, which had also been certified as PCI DSS compliant.[166]

These incidents raise the question of what benefit there is to payment card network participants of becoming PCI DSS compliant. PCI DSS compliance is extremely expensive, but might not ultimately protect them from data breaches and liability for the expenses caused by the breach, including reissuance of cards.[167]

As a concept, inter-network security coordination for payment systems makes sense. The PCI SCC is designed to facilitate coordination between competing payment card networks. This is an important goal, with potentially precompetitive effects through positive security externalities. Nevertheless, the PCI SCC's structure raises serious antitrust concerns. In execution, PCI DSS might be skewed by the dynamics of payment card network economics as well, and reflect the interest of issuers—the most price elastic type of network participant—rather than the overall interests of all network participants. In other words, the structure of the PCI SCC raises concerns that PCI DSS is being used to bolster the pre-existing problems in the payment card interchange fee system.

Given the significant benefits that can come from data security standard setting, standard-setting processes should be encouraged. But it is also important that they be fair. Standard setting needs to be a tool to further

---

161. *See* DISCOVER MERCHANT OPERATING REGULATIONS, *supra* note 67, §§ 4.1.3, 7.1.5.

162. *See* Sullivan, *supra* note 1, at 119.

163. Indictment at 3, United States v. Gonzalez, No. 09-cr-00626-JBS (D. N.J., Aug. 17, 2009); Kim Zetter, *TJX Hacker Charged with Heartland, Hannaford Breaches,* WIRED (Aug. 17, 2009, 2:34 PM), http://www.wired.com/threatlevel/2009/08/tjx-hacker-charged-with-heartland.

164. Alex Goldman, *Heartland Hit With $12M Breach Tab*, INTERNETNEWS.COM (May 8, 2009), http://www.internetnews.com/security/article.php/3819596; Jaikumar Vijayan, *Heartland Breach Shows Why Compliance Is Not Enough*, PC WORLD (Jan. 6, 2010, 11:15 AM), http://www.pcworld.com/article/186036/heartland_breach_shows_why_compliance_is_not_enough.html; Zetter, *supra* note 163.

165. Linda McGlasson, *Heartland Data Breach: Visa Questions Processor's PCI Compliance*, BANKINFO SECURITY (Mar. 24, 2009), http://www.bankinfosecurity.com/articles.php?art_id=1309.

166. Linda McGlasson, *Top 9 Breaches of 2009*, CU INFO SECURITY (Dec. 14, 2009), http://www.cuinfosecurity.com/articles.php?art_id=2001&pg=1.

167. *See* Steven Mott, *Why POS Merchants Don't Buy into Payment Security*, DIGITAL TRANSACTIONS (Sept. 7, 2007), http://www.digitaltransactions.net/index.php/news/story/1503.

competition, not to squelch it. This suggests two seemingly contradictory regulatory interventions: encouragement of inter-network coordination for data security setting and more vigorous antitrust enforcement. Standard setting should be encouraged, but only with a more adequately representative and fair governance structure that provides a balance of interest and due process.

The precise mechanics of a reformed payment system security standard setting are beyond the scope of this Article, but given the critical infrastructure utility role that payment card networks play in commercial transactions and the law enforcement resources involved, some level of government involvement to ensure that standards are set through a fair process that produces socially optimal outcomes is appropriate.[168] Already, the Durbin Interchange Amendment provides for the Federal Reserve to consider fraud prevention costs and technology in its rule-making regarding debit card interchange fees.[169]

Government involvement in payment card data security need not mean government setting of security standards. Instead, the involvement could be limited to government supervision of process. Because of its lack of formal procedural requirements, the PCI DSS standard setting process should be relatively nimble, but this comes at the expense of due process and adequate representation of all constituencies involved in payment card transactions, including merchants, consumers, and law enforcement. Payment card data security needs coordination between ostensible competitors, but if such coordination is to be permitted, it must be through a process that does not allow competing networks to leverage security standard setting to further their own economic interests at the expense of optimal security standards.

C. MORE VIGOROUS PAYMENTS ANTITRUST POLICY

The other concurrent approach that should be pursued is to improve inter-network competition for merchants' business. As the situation currently stands, networks compete with each other primarily for issuers, not for merchants. The goal of networks is to increase network transaction volume, and that requires getting as many of their cards in circulation as possible. Maximizing cards in circulation requires vigorous recruiting of issuers.

Once a network signs up issuers, it will get its cards out to consumers, and once a consumer presents the network's card at a merchant, the network

---

168. Carl Cargill & Sherri Bolin, *Standardization: A Failing Paradigm*, *in* STANDARDS AND PUBLIC POLICY 296, 312, 316 (Shane Greenberg & Victor Stango, eds., 2007) (arguing that standards are an "impure public good" which justifies government intervention when private standard setting processes fail).

169. Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, Pub. L. No. 111-203, § 1075(a)(2), 124 Stat. 1376, 2068–74 (2010) (amending § 920 of The Electronic Fund Transfer Act).

has a monopoly on processing the transaction. This means that the networks do not have to court merchants as assiduously as they do issuers. To be sure, a merchant can opt-out of accepting a particular network's cards, and some do, particularly for American Express;[170] but as long as the credit and signature networks all price fairly similarly for credit, signature debit, and PIN debit, respectively, there is no reason for a merchant to take one network brand and not another. Moreover, the complexity of interchange rates makes it difficult for merchants to even determine what relative pricing is between networks, as pricing depends on the type of card and the level of rewards, as well as the merchant's industry.[171] Because card network competition has focused on competition for issuers, rather than both issuers and merchants, the cost of payment card acceptance, including fraud liability, is structured to favor issuers.

The Durbin Interchange Amendment will change this situation by creating more competition for merchant business—but only for debit cards and small dollar credit card transactions. The Durbin Amendment requires that debit card interchange fees be "reasonable and proportional to the cost incurred by the issuer," meaning the incremental cost of a transaction, with an issuer-specific adjustment for fraud prevention costs, as determined by the Federal Reserve.[172] This provision could result in debit interchange pricing that strongly encourages the use of PIN or Chip & PIN technology; regulatory intervention might accomplish the optimal end that private-ordering has failed to do. It will take the outcome of the Federal Reserve's rule-making, to be finalized in early 2011,[173] before the ultimate effect is clear.

The Durbin Amendment also permits merchants to offer discounts (including in-kind discounts) to incentivize consumer use of particular payment systems;[174] and, critically, the Durbin Amendment forbids network exclusivity on debit cards and lets merchants choose the routing of debit transactions.[175] Thus, debit cards will be capable of "multi-homing"—clearing over multiple networks,[176] and merchants, rather than issuers, will decide which networks. The result should be that networks have to compete more for merchant routing decisions, which means lowering costs, be it direct pecuniary costs like interchange fees or indirect costs like fraud

---

170. *See* Meghan Boyer, *Discover Striving To Raise U.S. Merchants' Awareness Of Card-Acceptance Abilities*, PAYMENTSSOURCE, Apr. 21, 2010, http://www.paymentssource.com/news/-3001446-1.html.

171. *See* Levitin, *Economic Costs*, *supra* note 19, at 1323.

172. Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, Pub. L. No. 111-203, § 1075(a)(2), 124 Stat. 1376, 2068–74 (2010) (amending § 920 of The Electronic Fund Transfer Act).

173. *Id.* § 1075(b)(1)(A).

174. *Id.* § 1075(b)(2)(A).

175. *Id.* § 1075(b)(1)(A).

176. *Id.* § 1075(b)(1)(B).

liability. The Durbin Amendment is likely to affect not just debit cards, but also credit cards to the extent that credit competes with debit for small ticket transactions.

The Durbin Amendment is not a complete solution to the competition problems in the payment systems marketplace, but it opens the door to a rationalization of the fraud liability rules for merchants and issuers.

IV. LIMITATIONS OF CONSUMER LIABILITY: A DEFENSE

A. CONSUMER LIABILITY RULES FOR UNAUTHORIZED PAYMENT CARD TRANSACTIONS

The most major federal intervention in payment system loss allocation is the limitation by federal law of consumer liability for unauthorized transactions.[177] Consumer liability for unauthorized credit card transactions is limited to $50, and the consumer has no liability once the consumer has notified the card issuer about the loss, theft, or possible unauthorized use of the card.[178] The burden of proof to show that the use was authorized is on the card issuer.[179]

For debit cards, consumer liability is generally limited to $50,[180] but it increases to a maximum of $500 if the consumer does not notify the issuer within two business days of learning of the loss or theft of the card, and the card issuer establishes that the transactions would not have occurred had there been timely notice.[181] In addition, if the consumer does not report an unauthorized transaction that appears on a periodic account statement within sixty days of the transmittal of the statement, then the consumer incurs unlimited liability for all unauthorized transactions that occur between the end of those sixty days and notice to the issuer, provided that the issuer can show that the transactions would not have occurred had there been timely notice.[182] These time limits can be extended for extenuating circumstances, such as extended travel or hospitalization.[183] Again, in all

177. The legal definition of "unauthorized transaction" is somewhat different for credit cards and debit cards. *Compare* 12 C.F.R. § 226.12(b)(1) (2010) (defining "unauthorized use" as "the use of a credit card by a person other than the cardholder, who does not have actual, implied, or apparent authority for such use, and from which the cardholder receives no benefit"), *with* 15 U.S.C. § 1693a(11) (2010), *and* 12 C.F.R. § 205.2(m) (2010) (defining an "unauthorized electronic fund transfer" as "an electronic fund transfer from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit" and then noting several exceptions). These distinctions do not matter, however, for the purposes of this Article. *See* Gillette, *supra* note 8, at 200–02 (discussing the public choice issues with payment card liability limitation rules).

178. 15 U.S.C. § 1643 (2006); 12 C.F.R. § 226.12(b).

179. 15 U.S.C. § 1643(b).

180. 15 U.S.C. § 1693g(a) (2006); 12 C.F.R. § 205.6(b)(1) (2010).

181. 15 U.S.C. § 1693g(a); 12 C.F.R. § 205.6(b)(2).

182. 15 U.S.C. § 1693g(a); 12 C.F.R. § 205.6(b)(3).

183. 15 U.S.C. § 1693g(a); 12 C.F.R. § 205.6(b)(4).

cases, the burden of proof to show that a transaction was in fact authorized is on the card issuer.[184]

These rules apply to all unauthorized usage, not just fraud, which is the focus of this Article. The federal liability rules thus create something close to a strict liability regime for credit card fraud and a strict liability scheme with an exception for contributory negligence for debit cards.[185] It is worth noting that liability for unauthorized payment card transactions contrasts with checks, where there is no consumer liability for unauthorized transactions (meaning orders of payment) whatsoever, absent consumer negligence that "substantially contributes" to the fraud.[186] Whereas the checking system has a true contributory negligence scheme, credit cards are strict liability, and debit cards are strict liability with contributory negligence regarding the amount, but not the fact, of the loss.

B. THE CASE AGAINST MANDATORY LIABILITY RULES

Epstein and Brown contend that consumer liability for unauthorized transactions should not be capped by statute, as they "see no reason even for this (modest) restriction on freedom of contract. If payment card companies think larger penalties are appropriate and disclose such penalties to consumers, the losses should not be socialized as a matter of law."[187]

While Epstein and Brown's major complaint about the mandatory liability caps is that it could frustrate more efficient private bargaining over liability, that is not the only problem with the mandatory liability rules for unauthorized transactions. The mandatory liability rules also create a moral hazard and effectuate a wealth redistribution from consumers who engage in low-risk behavior to consumers who engage in high-risk behavior. The limitation on consumer liability, in most cases to $50 (which is not inflation indexed), provides little pecuniary incentive for consumers to take care in their transactions and with their cards. Moreover, given the difficulties in proving first-party fraud, with the burden of showing unauthorized transactions resting on the card issuer, the liability limitation creates a very real moral hazard of first-party fraud.

In addition, the liability rules create a perverse redistribution that rewards high-risk behavior. Low-risk consumers might prefer to incur more potential liability in exchange for savings on other payment card price terms. By being pooled with high-risk consumers under the same

184. 15 U.S.C. § 1693g(b).

185. There is a rich literature which considers the differences in fraud and error liability rules for different payment systems and whether they should be harmonized. *See supra* note 8.

186. U.C.C. § 3-401(a) (2006) (no liability on instrument without signature); *id.* § 3-403 (unauthorized signature on instrument is only effective as that of the unauthorized signer); *id.* § 3-406 (liability if negligence "substantially contributes" to fraud on instrument). Uniform Commercial Code Article 3 does not distinguish between consumer and nonconsumer drawers of checks.

187. Epstein & Brown, *supra* note 9, at 219.

mandatory liability rules, the low-risk consumers are being forced to forgo these potential savings for the benefit of high-risk consumers. The result is to penalize precisely those consumers whose behavior should be encouraged. In such circumstances, a rational consumer will be incentivized to engage in higher-risk behavior in order to be a recipient, rather than the payee of the subsidy.

Notably, MasterCard[188] and Visa[189] both have so-called "zero liability" policies that reduce consumer liability in many cases beneath the federal liability cap.[190] These caps essentially install a negligence regime for liability up to $50, after which the federal strict liability regimes take over. Epstein and Brown argue that the zero liability policies demonstrate that "[m]arket pressures have pushed the balance still further, insulating payment card users from essentially all fraud losses."[191] In other words, the federal law is an unnecessary (but fortunately harmless) intervention. Indeed, as Duncan Douglass has observed, the zero liability policy arguably creates a moral hazard, as consumers have little reason to take care to protect their cards and card data.[192]

C. IN DEFENSE OF THE CONSUMER LIABILITY LIMITATIONS

Despite the problems created by the mandatory liability caps, there is nevertheless a good case supporting them. Absent the mandatory caps, the zero liability policies might not obtain and adverse selection, disproportionate negotiation costs, information asymmetries, consumer hyperbolic discounting and optimism biases, the relative salience of different price points to consumers, and consumers' limited ability to absorb losses relative to other payment card network participants all militate for capping consumer liability.

1. Counterfactual Consideration

Epstein and Brown's reading of the impact of the zero liability policy is reasonable, but it is hardly the only fair interpretation. First, it is worth

188. Zero Liability, MASTERCARD, http://www.mastercard.com/us/personal/en/cardholder services/zeroliability.html (last visited Dec. 30, 2010).

189. Zero Liability, VISA, http://usa.visa.com/personal/security/visa_security_program/zero_ liability.html (last visited Dec. 30, 2010).

190. Bank of America offers its own "zero liability" policy. *See, e.g.*, Bank of America Merrill Lynch Visa® Reward Card Terms and Conditions, BANK OF AMERICA, https://prepaid.bankofamerica.com/RewardCard/PRC384/CP384-T00-002/docs/terms.htm (last visited Dec. 30, 2010). It is important to remember that the stated zero liability policy is not zero liability. It is conditional on the cardholder having taken reasonable care (in the issuer's view), the cardholder having had no more than two other incidents in the last year, and the cardholder's account being "in good standing." *See, e.g.*, MASTERCARD RULES, *supra* note 67, § 3.11(2), at 15-7 (conditions governing cardholder liability in the United States). Zero liability is great marketing, but it is not clear how often it is really zero liability.

191. Epstein & Brown, *supra* note 9, at 219.

192. Douglass, *supra* note 9, at 46.

considering a counterfactual scenario. What would the world look like without the federal $50 liability limitation on credit cards? Would Visa and MasterCard have adopted zero liability policies? Maybe. The zero liability policy was only adopted in 2000,[193] which indicates that it might have been a move to encourage e-commerce.

But it might also be that once consumer liability is limited to $50, the marketing benefits to the network of going from $50 liability to zero liability for nonnegligent consumers outweigh the fraud losses. Given the costs of pursuing the last $50 of liability, issuers really do not give up anything by going to zero liability, and they gain a significant marketing benefit. The zero liability policies are advertised in a way that implies that they are strict liability regimes, with the fact that they are highly discretionary negligence regimes hidden in vaguely worded fine print. Thus, consumers might well assume that they have less liability than they do under the zero liability policies. Moreover, the cost of disputing *up to* $50 with consumers might simply not be worthwhile for issuers.

The real question is whether networks would adopt zero liability policies if by statute consumers were liable for $100 or $500 or $1,000? We don't know, but it cautions against assuming that the $50 liability limit has been toothless or that zero liability would be the policy the networks would generally adopt.[194]

2. Monetary Deductibles, Copayments, and Contributory Negligence

The mandatory liability caps are part of a system that includes notable moral hazard mitigants. The federal consumer liability limitations are a type of strict liability regime for card fraud. As Samuel Rea has noted, "[s]trict liability without contributory negligence is essentially mandatory insurance."[195] A standard insurance move to reduce moral hazard is to require deductibles and copayments. The $50 liability cap on credit cards

193. Letter from Russel W. Schrader, Visa U.S.A., to Fed. Trade Comm'n (Sept. 15, 2000), *available* at http://www.ftc.gov/bcp/workshops/idtheft/comments/schraderrussellw.pdf (discussing Visa's zero liability policy that took effect on April 4, 2000); Selco Visa Cards—Zero Liability, SELCO, https://www.selco.org/creditcards/zero.liability.asp (last visited Sept. 23, 2010); Eden Jaeger, *Should You Be Afraid of Your Debit Card?*, FINANCE & FAT (Jan. 4, 2008), http://www.financeandfat.com/archives/should-you-be-afraid-of-your-debit-card.

194. One factor that might push for some sort of liability limiting policy even in the absence of the federal caps is the recognition that consumer loss aversion is a major obstacle to increasing the use of payment cards. Would consumers have adopted payment cards on as wide of a scale as they have without the federal liability caps? We cannot be sure, but it seems likely that the liability caps at least contributed to greater consumer adoption of payment cards, and by further reducing the caps the card networks aimed to eliminate the residual loss aversion.

195. Samuel A. Rea, Jr., *Comments on Epstein,* 14 J. LEGAL STUD. 671, 672 (1985); *see also* Gillette, *supra* note 8, at 201 (discussing liability cap as insurance).

can thus be seen as equivalent to a $50 deductible on a mandatory federal insurance policy.[196]

For debit cards, federal law creates a strict liability regime with a peculiar kind of contributory negligence. The contributory negligence under the Electronic Funds Transfer Act and Reg E is only for losses incurred *after* the loss or theft of the card due to failure to promptly report the loss or theft; it does not apply to pre-loss or pre-theft behavior.[197] In other words, the contributory negligence component of consumer liability for unauthorized debit card transactions only goes to the magnitude of the loss due to unauthorized use, not the actions that caused the loss in the first place. The result is that it does not incentivize consumers to take precautions to prevent loss or theft. This means that in terms of fraud losses, there is primarily a strict liability regime for debit cards too, and with a $50 deductible.

3. Non-Pecuniary Costs

In addition to the monetary deductible, there can also be considerable non-pecuniary harms to consumers from unauthorized card usage. It is not merely "the major inconvenience of the disruption of service,"[198] or having to get the charges reversed, but also things like having to monitor credit reports, close other accounts, etc.[199] These additional, non-pecuniary costs are essentially copayments. Thus, built into the federal liability limitation are two standard responses to moral hazard problems—deductibles and copayments.

4. Limited Consumer Ability to Prevent Fraud

Imposing liability on consumers for unauthorized transactions makes little sense if that liability does not alter consumer behavior. Some unauthorized transactions are due to consumer negligence, but others are not. We lack an empirical sense of the role cardholder negligence plays in unauthorized transactions. Clearly there are numerous fraud possibilities even when a consumer acts responsibly. Consider a simple case where a

---

196. One can, of course, argue whether that is a sufficiently large deductible to ensure optimal care, not least given that the $50 liability limit is not inflation adjusted and has remained constant for decades.

197. *See* 12 C.F.R. § 205.6(b)(2) (2010).

> Negligence by the consumer cannot be used as the basis for imposing greater liability than is permissible under Regulation E. Thus, consumer behavior that may constitute negligence under state law, such as writing the PIN on a debit card or on a piece of paper kept with the card, does not affect the consumer's liability for unauthorized transfers.

Id. § 205, at Supplement I to Part 205, Official Staff Interpretations, ¶6(b) (2).

198. Epstein & Brown, *supra* note 9, at 219.

199. *See* Mann, *Making Sense of Payments*, *supra* note 8, at 638.

consumer is robbed and the card is used for a transaction by the thief before the consumer can report its loss. What justification is there for consumer liability then? More typically, card data is not stolen directly from the consumer, but from a merchant or a financial institution. Again, the justification for consumer liability is missing in such cases; the consumer has no ability to control merchant or financial institution data security measures.

Instead, the case for consumer liability seems limited to situations in which a consumer fails to take reasonable care of his or her physical card, such as writing a PIN number on a debit card and then leaving a debit card in a location where it could be pilfered by a domestic employee. It seems unlikely that such situations account for a significant portion of payment card fraud.

Consider, then, an intermediate situation, in which the cardholder leaves his card out long enough for someone to copy down the card digits. Should the cardholder be liable in such a situation? Or should the liability be better placed on the card issuer that issued an account access device that is so easily compromised?

5. Consumer Knowledge of Liability Rules and Concerns About Issuer Compliance

In addition, as Professor Ronald Mann has noted, consumers may not know of the liability limitation.[200] It is doubtful, for example, that most consumers are aware of the contributory negligence rules for debit card liability. Similarly, Mann notes that even informed consumers might doubt whether financial institutions would comply with the law.[201] If a financial institution does not comply with the liability rules in the case of a debit transaction, the consumer simply loses his or her money. In the case of a credit transaction, the consumer might be able to avoid the monetary loss, but risks the loss of a credit line, a damaged credit report, and debt collection harassment. While the consumer could litigate the issue, in many cases, the cost of litigating would vastly outweigh the harm to the consumer.[202]

When consumers are unaware of the liability limitation, moral hazard simply will not exist, and if they are concerned about legal compliance, then moral hazard must be discounted. All of these factors—deductibles, copayments, contributory negligence, lack of knowledge about the law, and doubts about compliance with the law—suggest that moral hazard concerns

200. *Id.*; *see also* Cooter & Rubin, *supra* note 8, at 75 ("Liability, however, is a useful incentive, whether for precaution or innovation, only to the extent that behavior responds to it; a particular assignment of liability that does not influence behavior has no economic justification.").

201. Mann, *Making Sense of Payments*, *supra* note 8, at 638.

202. *See* Cooter & Rubin, *supra* note 8, at 81.

about the federal liability limitation are overblown, and that consumers have a reasonably strong incentive to protect their cards and card data.

Finally, while the zero liability policy could create a moral hazard if the counterweights of deductibles and copayments were insufficient, that moral hazard must be weighed against the alternative. We have to consider the situation that would obtain in the absence of the zero liability policy or $50 federal liability cap. What would consumer liability look like? Would it reflect a Coasean bargain between consumers and card issuer? It is hard to believe that it would because of the tremendous information asymmetries between card issuers and consumers.[203]

6. Adverse Selection as Justification for Mandatory Liability Rules

Information asymmetries raise the possibility of adverse selection problems, which are a standard justification for mandatory insurance regimes like the federal consumer liability limitations. (An analogous consumer liability situation is state law mandating nonrecourse mortgages.[204]) The problem of adverse selection arises because of a tendency of low-risk individuals to drop out of insurance pools when insurers cannot distinguish between high- and low-risk individuals.[205] Insurers must charge a blended price, which is too high for the low-risk individuals. The result is that insurance pools are then comprised of higher risk individuals, so insurers charge higher premiums, which further exacerbates the adverse selection by driving out the lower-risk individuals remaining in the pool. The result can be a socially suboptimal level of insurance.

A standard response to adverse selection is to mandate insurance, so as to force both low-risk and high-risk individuals into the same risk pool.[206] In the case of payment card fraud, there is good reason to encourage mandatory insurance. There is a possibility of suboptimal insurance due to consumers' difficulty in gauging both the likelihood and magnitude of payment card fraud loss because neither relates solely to their behavior. To the extent that consumers overestimate the risks, they may well opt-out of using payment cards altogether. Liability limitations are a market confidence building measure.

---

203. *See id.* at 68–70 (discussing the problems of information asymmetries in payment markets, wherein financial institutions typically have superior information to consumers).

204. I am indebted to Professor Ron Harris of Tel Aviv University School of Law for this insight, which comes from his work-in-progress on nonrecourse mortgages.

205. Tom Baker, *Containing the Promise of Insurance: Adverse Selection and Risk Classification, in* RISK AND MORALITY, RICHARD V. ERICSON & AARON DOYLE, EDS. 258, 259, 261 (2003). *But see* Peter Siegelman, *Adverse Selection in Insurance Markets: An Exaggerated Threat*, 113 YALE L.J. 1223 (2004).

206. *See* Rea, *supra* note 195, at 673.

7. Contractual Frictions: Information Asymmetries, Bargaining Costs, Bundled Pricing, Hyperbolic Discounting, and Price Salience

Adverse selection is driven by one set of information asymmetries—that consumers know more about their own riskiness than card issuers. Another set of information asymmetries—that issuers know more about the terms of cardholder agreements than consumers—combines with asymmetric negotiation costs to create further frictions that impede efficient Coasean bargaining. As Professors Cooter and Rubin have noted:

> [T]he cost of negotiating the loss allocation provisions of a consumer deposit agreement typically exceeds the potential benefit. Shopping for alternative sets of fixed term contracts—a more realistic scenario than bargaining for specific terms—eliminates these negotiation costs, but replaces them with search costs. Moreover, asymmetric information limits the effectiveness of consumer shopping. Consumers are unlikely to think about the liability terms of a contract when opening an account, and those that do, find their curiosity rewarded with the incomprehensible legalisms of form contracts and statute books. Even if they knew what the terms meant, consumers generally would not know how to value differences in these terms.[207]

A further reason to be skeptical that private bargaining would produce optimal consumer liability rules is that liability for unauthorized transactions is only one term among many in cardholder agreements.[208] If one takes Epstein and Brown's subscription to a Coasean universe seriously, this observation should be heartening. It should not matter what the fraud liability rule is because the parties can simply reallocate if that is efficient.[209] Liability for unauthorized use is merely one component of payment card pricing. Thus, the federal liability cap does not restrict total pricing of payment cards. It only affects one way of expressing that price. Accordingly, parties can effectively reallocate the total price through other price components of payment cards. In the Coasean world, whether the price of using a payment card is allocated via liability rules or annual fees or interchange fees should not matter if there is the same level of competition on each and every price term. In other words, if Epstein and Brown are correct about the market, the federal liability cap does not create a troublesome distortion.

---

207. Cooter & Rubin, *supra* note 8, at 68–69.

208. Oren Bar-Gill, *Bundling and Consumer Misperception*, 73 U. CHI. L. REV. 33, 33–35 (2006).

209. *See generally* Coase, *supra* note 15.

In reality, however, not all price terms for payment cards are equal and fully interchangeable. There is more vigorous competition on some price terms than others, in part due to their salience to consumers. When confronted with a multi-term contract, consumers may give undue emphasis to terms that are particularly salient either because of the manner in which the information is presented to the consumer or because of hyperbolic discounting of contingent events.[210] This means that there is a discounting that occurs in the trade-off between price terms, so the reallocation of costs among price terms might not be neutral in terms of total cost. If payment card pricing is forced by regulation from less salient to more salient price terms, there will be more vigorous price competition, which will push down the total cost of using a payment card.

This suggests that in the absence of regulation, a profit-maximizing firm will place as much of the price as possible on less salient terms and will max out on consumers' price elasticity on less salient terms before letting pricing spill over to more salient terms. Regulation, then, does not necessarily result in a one-for-one substitution of price terms, but can result in an overall reduction in price (and profit margin).

The contingent nature of liability for unauthorized card usage, as well as the potential absence of a clear monetary price term if either a consumer negligence standard or strict consumer liability were to apply, means that fraud liability is unlikely to be a salient term for consumers.[211] In the context of these bundled contracts, there might not be optimal pricing of fraud terms, even if there were vigorous competition among issuers for consumers. Thus, the federal liability cap might actually have precompetitive effects by forcing payment card issuers to shift pricing away from a less salient term like liability for unauthorized use and to more salient price points like annual fees or interest rates.

The federal statutory limitations on consumer liability may not be optimal (not least because the $50 deductible is not inflation indexed, so the real potential pecuniary liability is constantly decreasing), but it is far from clear that they result in an inferior outcome than private-ordering. The regulatory outcome may not be Kaldor-Hicks optimal, but it might increase consumer surplus by encouraging more vigorous price competition.

8. Relative Ability to Bear Losses

A final argument for the federal liability cap is distributional, or as Cooter and Rubin refer to it, the "loss spreading principle".[212] Once there

---

210. *See, e.g.*, Els C. M. van Schie & Joop van der Pligt, *Influencing Risk Preference in Decision Making: The Effects of Framing and Salience*, 63 ORG. BEHAV. & HUM. DECISION PROCESSES 264 (1995).

211. Cooter & Rubin, *supra* note 8, at 70 ("Consumer payment contracts contain elements other than loss allocation terms, but market failure is most likely to involve these technical, obscure elements of the contract, rather than the comprehensible and salient ones.").

212. *Id.* at 70–73.

are losses in the system, they must be allocated somewhere, and placing losses on parties in accordance with their ability to absorb losses presents a potential principle for loss allocation. The loss spreading principle stands in some tension with a least cost avoider principle, as it is based on ability to absorb, rather than prevent, losses.

Cooter and Rubin argue that risk should be assigned to the party that can achieve risk-neutrality—that is having equal valuation of a risk of a loss and the average value of that loss—at the lowest cost.[213] As Cooter and Rubin explain, risk neutrality is dependent upon the relative size of the loss to a party's assets and the party's ability to spread the loss.[214] Both factors point to financial institutions and merchants being able to achieve risk neutrality more cheaply than consumers.

Because consumers' resources are generally more limited than financial institutions' or merchants', consumers are less well suited to bear unlimited liability from the unauthorized use of a payment card than a financial institution or a merchant. Liability for $100,000 in unauthorized charges would be devastating to most households' finances in a way that it would not be for a financial institution or certainly a large merchant. This makes consumers more risk averse than financial institutions or merchants.

Consumers also have less ability to spread losses than financial institutions or merchants. For a consumer, the unauthorized use of a payment card is a fairly remote risk, but with potentially high costs. These costs will likely be borne entirely by the consumer; they cannot easily be passed on to other parties.[215] For a financial institution or a merchant, fraud is a regular occurrence, and its costs can be amortized over a large base of transactions. Moreover, because financial institutions and merchants have superior information about their risks from payment card fraud relative to consumers, they are more likely to optimally insure against it.[216] Consumers' more limited ability to absorb losses than other payment card network participants is an additional argument for limiting their liability by statute.

CONCLUSION

Payment card networks, if left to their own devices, are as likely to produce private disorder, as efficient private order. Regulatory attention has focused on the explicit price points in payments—interchange fees—but the latent price point of fraud liability allocation is equally important. Optimizing fraud liability allocation necessitates recognition of the co-

213. *Id.* at 71.
214. *Id.*
215. Consumers are unlikely to insure against losses because the risk is difficult to estimate, which results in known bargaining costs outweighing the questionable benefit of the insurance. *Id.* at 72.
216. *Id.* at 72-73.

optetive nature of payment card networks. Some issues are best approached through encouraging fairer and more adequate representation of all parties in interest in coordination among payment card networks. Other issues are best approached through encouraging more vigorous competition. We should not assume that the invisible hand will guide the payment card industry to the optimal outcome; but with limited regulatory corrections, payments card network liability rules can come closer to achieving a Coasean paradise, and making payments—the ultimate unavoidable transaction cost—more efficient, thereby reducing transaction costs throughout the rest of the economy.