Cybersecurity in the Payment Card Industry

Richard A. Epstein[†] *& Thomas P. Brown*[††]

I. THE TWO-TIER LOGIC OF THEFT PREVENTION

The payment card industry has of late received an enormous level of critical academic scrutiny. The two issues that have dominated the literature are antitrust and consumer protection. The former deals with the various ways in which credit card companies structure themselves and their possible exposure to charges of monopolization. The latter deals with various forms of legislation that ask whether, and if so how, state regulation should mandate disclosure on the one hand and limit the substantive terms of consumer contracts on the other. From our classical liberal perspective, we think that these two jumping-off points are odd places to begin the inquiry, given the high level of competition that exists everywhere in the credit card industry, both from established players and from new entrants.[1] Using a payment card (as opposed to some other form of payment) rests on voluntary decisions by consumers and merchants, as well as the banks with which they interact. Although it is theoretically possible to imagine government intervention improving on the outcome that these multiple parties are able to achieve through contract, in practice, a litany of political pressures and regulatory glitches make it highly unlikely that those results could be achieved.

This hands-off conclusion does not apply to another issue that has plagued private payment systems since their emergence a half-century

[†] James Parker Hall Distinguished Service Professor of Law, The University of Chicago and Peter and Kirsten Bedford Senior Fellow, The Hoover Institution.

[††] Partner, O'Melveny & Myers. Both authors have consulted for Visa Inc. But our views on this subject are our own. We thank Chad Clamage, Stanford Law School, Class of 2008, and Ramtin Taheri, The University of Chicago Law School, Class of 2009, for their valuable research assistance on earlier drafts of the article.

[1] For our view on the antitrust issue, see generally Richard A. Epstein and Thomas P. Brown, *The War on Plastic*, 29 Reg 12 (2006) (arguing that markets provide sufficient rate regulation and that antitrust threatens to stifle the competition that it seeks to foster); Richard A. Epstein, *Behavioral Economics: Human Errors and Market Corrections*, 73 U Chi L Rev 111 (2006) (analyzing consumer-credit behavior and concluding that even devotees of a soft form of paternalism should propose no protection beyond that which a truth-in-lending law affords against misleading representations); Richard A. Epstein, *The Regulation of Interchange Fees: Australian Fine-tuning Gone Awry*, 2005 Colum Bus L Rev 551 (analyzing the Reserve Bank of Australia's attempt, and ultimate failure, to impose credit rate restrictions and arguing that voluntary arrangements supply superior alternatives to antitrust regulation).

ago—fraud and, closely related, identity theft.[2] As issues go, fraud is generally an unpopular topic for academics and regulators. Virtually everyone agrees that innocent transactors should be protected against the fraudulent actions of third parties. But at that point the conversation generally ceases, without undertaking the hard work to find what contractual and institutional arrangements work best to combat the fraud that everyone deplores. If fraud is bad, then what mix of public and private systems should be used to implement a coherent policy of fraud prevention in modern payment transactions, all of which involve the extensive creation, transmission, storage, and use of information, both financial and personal, involving huge numbers of individuals?[3]

The logistical problems that are raised by dealing with the massive and continuous flow of transactions should, we think, be virtually self-evident. But the basic risks to these voluntary transactions are as old as commerce itself. Even the earliest legal sources take for granted the corrosive effect of fraud and theft in their efforts to combat it. We briefly review the evolution of the law of theft, the punishment of which remains a proper government function, in order to set the stage for dealing with the contractual and regulatory issues that remain.

II. QUICK TOUR OF THE LAW OF THEFT

Much of the modern law on cybersecurity is shaped by the earlier law on theft and related offenses. The Roman law of *furtum*, for example, defined the notion of theft very broadly, so as to include not only the removal of chattels from the possession of their owner, but also any knowingly unauthorized use of a thing by a bailee or other servant who took possession from the owner.[4] The penalties for theft were harsh, calling initially for death.[5] The Roman law of theft did not only address the behavior of the thief. It also brought within the scope of the wrong those individuals who received the stolen property with

[2] We thus largely exclude from this discussion other important dangers that include denial of service attacks, viruses, and loss of state secrets.

[3] For a discussion of currently accepted models for addressing data leaks, see Paul M. Schwartz and Edward J. Janger, *Notification of Data Security Breaches*, 105 Mich L Rev 913, 932–45 (2007) (arguing that current models are insufficient and advocating for the creation of a coordinated response architecture as well as a critical organization monitoring credit security performance).

[4] For the relevant materials, see Gaius, *The Institutes of Gaius*, bk III, §§ 195–97 at 219 (Clarendon 1946) (Francis de Zulueta, ed). For a general discussion, see Barry Nicholas, *An Introduction to Roman Law* 211–15 (Clarendon 1962) (lamenting the complexities of the Roman law of theft, detailing the offense's particular history, and explaining the distinctions between different theft offenses).

[5] Gaius, *The Institutes of Gaius* bk III, § 189 at 215–16 (cited in note 4) (stating that the penalty for theft was capital and required enslavement to the person from whom the thief had stolen or, if the thief was a slave, death).

knowledge of the theft.[6] The obvious point for this regime was to shrink the incentive for theft by reducing the prospects of sale in a secondary market. That in turn reduces the gains from theft when the value in exchange is greater than it is in use, which is typically the case for stolen property.

For its part, the early English law of theft tied the offense not to the wrongful misappropriation of a particular chattel, but to the taking of the chattel from the possession of the owner with an intention permanently to deprive him of its possession.[7] That definition proved less durable than the earlier Roman definition, so that additional offenses—larceny by trick, larceny by bailee, taking by false pretenses, and embezzlement—had to be grafted onto this paradigm case to close the gap.[8] In more modern times, as information became more important, theft was no longer applied exclusively to tangible chattels. Definitions in the Model Penal Code, for example, have been expanded to make theft statutes cover various forms of intangible property,[9] including of course the databases that are everywhere today protected as a form of trade secret, which themselves are now subject to stringent forms of federal legislation that call for criminal penalties, including fines, imprisonment, and forfeiture.[10] The federal statute also extends its prohibitions to anyone who "receives, buys, or possesses" such information.[11]

The persistent expansion of the modern law of theft represents, of course, an effort to stop antisocial behavior by the use of criminal sanctions against the wrongdoer or wrongdoers involved first in taking and thereafter in dealing with stolen goods or information. Yet at the same time, public force has never been the only weapon used to counteract theft. A second task, of equal importance, is the allocation of the risk of loss among *innocent parties* who have suffered losses from

[6] Id bk III, §§ 186–87 at 214 (distinguishing between *furtum conceptum*, where a stolen thing has been sought and found on a man's premises in the presence of a witness, and *furtum oblatum*, where a stolen thing has been passed off by someone and has been found on a man's premises rather than his own).

[7] For an exposition of the evolution of larceny away from its roots in trespass, see generally George P. Fletcher, *The Metamorphosis of Larceny*, 89 Harv L Rev 469 (1976) (arguing that the transformation from the common law has expanded the range of circumstances that can provoke intrusive prosecutorial scrutiny).

[8] For the variations, see Model Penal Code § 223.1(1) (ALI 1962) (calling for the consolidation of theft offenses).

[9] Id § 223.0(6) (defining property as anything of value).

[10] See Economic Espionage Act of 1996, Pub L No 104-294, 110 Stat 3488, codified as amended at 18 USC §§ 1831–39 (2000 & Supp 2002) (broadly covering the conversion of trade secrets "related to or included in a product that is produced for or placed in interstate or foreign commerce," which covers just about every commercial secret). For an explanation of fines and imprisonment, see id § 1832(a). For criminal forfeiture, see id § 1834.

[11] Id § 1832(a)(3).

various forms of theft. The usual rule starts with the simple proposition that in the first instance, the loss from theft falls directly on the owner of the property, who then has a set of strong private incentives to guard against that theft. The level of private precautions will of course reflect the effectiveness of the public law in preventing theft, such that in the extreme no one would so much as lock his gates if the public sanctions against theft were perfect. But it becomes evident that when these sanctions fall short, private individuals will take precautions that start with doors and progress to elaborate security systems designed to guard against theft. At this point all actors engage in a delicate coordination game: if public authorities reduce or redirect their level of protection, private individuals will undertake additional steps for self-protection. It is therefore difficult in the abstract to judge either the relative or combined effectiveness of the two systems in preventing loss. The plot thickens when, as is common in many cases, the property stolen is subject to the divided control of two or more individuals, as when a chattel is stolen from a party to whom it has been lent. The problem of divided control, moreover, is far more critical with information than it is with tangible objects, for the simple reason that the same information is routinely shared by large numbers of individuals in ordinary cases, as is necessarily the case with routine credit information.

In these cases, it is critical to determine how to divide the risk of loss between the multiple parties. In the early Roman and English systems, the allocation was often determined by an explicit rule that depended both on the nature of the divided ownership and the actual source of the loss.[12] In transactions for the benefit of the bailee, the risk of loss was presumptively placed on him. But when the transaction was for the benefit of the bailor (as in bailments for deposit), the risk of loss would normally lie on the owner of the property. The analysis was further complicated depending on the source of the loss. A bailee who was required to take precautions against simple theft might not be required to take them against robbery. In more complicated situations, especially those involving three or more parties, the allocation of loss between the parties could be determined by contract, which could override the presumptive allocation of loss set by any default rule. These contracts did not emerge in early times, and for two reasons. The default rules usually offered an accurate assignment of the risk of loss in routine transactions, and the size of the transac-

[12] For the Roman rules, see Gaius, *The Institutes of Gaius* bk III, §§ 203–08 at 221–22 (cited in note 4) (explaining that a theft action is available to those who have an interest in the safety of the thing stolen, including collateral interests).

tion was not large enough to warrant any private revision of the initial loss provisions. But in all settings, the debates were only instrumental, and never moral: the object of choosing the right rules for risk allocation was to minimize the *net* costs of theft, as measured by the losses from the theft, less the costs of prevention, including the costs of running the system. In principle, the usual marginal conditions should hold, such that the last dollar spent on theft prevention should reduce the losses from stolen property by one dollar—a standard that is hard to implement in practice, when there are so many moving margins at any one time.

III. The Two Tiers in Payment Card Markets

We think that this basic two-part program carries over without missing a beat to the various financial losses that are associated with payment card transactions. Payment card transactions involve the coordination of activity across many different parties. A "simple" transaction frequently involves five parties—the cardholder, the merchant, the cardholder's bank, the merchant's bank, and a network connecting the two financial institutions. When a cardholder swipes a card at a merchant through an electronic terminal, the terminal captures the information on the back of the card, adds information about the transaction and relays the information to the network associated with the card. The network performs a screen (for example, confirming that the card is genuine) and, assuming the transaction passes that test, asks the cardholder's bank to authorize the purchase. The cardholder's bank checks to see whether the cardholder has sufficient funds in the account to cover the purchase. If the cardholder has funds available to cover the purchase, the cardholder's bank generally approves the transaction and relays the approval back up the chain to the merchant.[13] The entire process takes a couple of seconds.[14] Each link in the approval process relies on information that originates with the card presented by the cardholder, making the cards and the information they contain inherently valuable.

[13] The text describes a typical Visa or MasterCard card transaction. See David S. Evans and Richard Schmalensee, *Playing with Plastic: The Digital Revolution in Buying and Borrowing* 9–10 (MIT 2d ed 2005). American Express and Discover transactions omit a couple of steps in the approval process by dealing directly with merchants and cardholders.

[14] Over the last thirty years, a highly specialized payment business in the United States has developed, which relies on third-party data processors to help banks on both the cardholder and merchant sides. The increase in the number of parties to a transaction to seven decreases the total processing time. See id at 247–51 (discussing the evolution of payment processing and identifying the different entities involved in a payment card transaction).

There is little doubt today that extensive criminal sanctions are properly imposed on those who steal valuable payment card information. But prosecution is not an easy job. The thefts, as we shall see, are often made surreptitiously and at a distance. Their clever execution makes prosecution of the thieves, many of whom operate across the globe, a difficult matter requiring the coordination of law enforcement officials from many nations. The thieves, moreover, always work diligently to keep the fact of the theft hidden from the person from whom the data was stolen in order to prolong the use of the stolen information. Once the fact of the theft becomes known to the person from whom the data was stolen, public disclosure is simply a matter of time, and at that point, the stolen data lose most, if not all, of their value to the thief. No one doubts that investigating and prosecuting thieves of payment card information is worth undertaking; how these investigations should be done, or the various criminal sanctions imposed lie, however, beyond the scope of this paper.

Instead, this paper addresses the second strategy of loss prevention: the private arrangements among the various persons against whom the theft has been perpetuated. Initially, it should be clear that the optimal structure of loss prevention in this area is far more complex than it is with the traditional theft of chattels, or indeed, even with various kinds of trade secrets, for the reasons noted above. The simple point here is that the process of entrustment with information is not what it is for chattels. A chattel can be given to one person for safekeeping, so that the owner can use personal knowledge to limit loss. But that option is not available with information that has to flow through multiple hands to be valuable. Universally, stolen payment card information is worthless to the thief unless it can be used to generate a transaction. In order to be used, however, the data must pass through each of the links in the payment card chain: the merchant through whom the thief tries to use the stolen data to generate a new transaction; the merchant's acquiring bank; the card network; the issuing bank; and, ultimately, the cardholder.

At least potentially, each link in the chain has an interest in blocking the attempted fraud. Depending on how the information associated with the payment card was obtained by the thief, some links may be better able to distinguish attempted fraud from a legitimate transaction. For example, did the consumer lose this card? Was the consumer's wallet stolen? Did the Russian mafia obtain the information encoded on the magnetic stripe on the back of this card by penetrating the system?[15] The structure of the typical credit card trans-

[15] For a discussion of the role of Russian mafia, see text accompanying notes 41–42.

action relies on a constant use of shared information, which means that it is highly unlikely that any one person or institution qualifies as *the* cheapest cost avoider. Accordingly, any rational approach to loss prevention requires the coordination of multiple actors up and down the chain of credit card use. And someone has to define the responsibilities for each link in the chain and decide what each link needs to know.

Our central thesis—which, except for recent developments, we would have thought beyond reproach—is that 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. For payment card information, the costs of keeping information secure and the benefits that flow from better security fall on the participants in the system. No public body outside the system is likely to have the information and ability to design a strategy for loss prevention that outperforms one that private parties can devise for themselves.[16]

We are under no illusion that this system will be perfect. Javelin Strategy and Research began reporting statistics on identity theft—broadly defined to include fraudulent use of information associated with existing payment cards—in 2003 with a report commissioned by the Federal Trade Commission (FTC).[17] Javelin estimated that total fraud in 2006 from identity theft was $49.3 billion.[18] This astounding number actually represents a decline from previous levels. Javelin estimated that total fraud resulting from identity theft was $53.8 billion in 2003.[19] Although Javelin's definition of fraud may overstate the actual losses from fraud, other sources confirm that the actual costs of fraud are significant, even under more restrictive metrics. According to the FTC, consumers reported credit card fraud losses of $1.2 billion in 2006, up significantly from 2005.[20] Financial institutions report fraud

[16] For a similar view about cybersecurity issues more generally, see Robert W. Hahn and Anne Layne-Farrar, *The Law and Economics of Software Security*, 30 Harv J L & Pub Policy 283, 286 (2006) (noting that the cure is often worse than the disease). For a somewhat different take, see Schwartz and Janger, 105 Mich L Rev at 960–70 (cited in note 3) (suggesting the need for a "coordinated response agent" to deal with information security concerns).

[17] For the latest version, see generally Mary T. Monahan, *2007 Identity Fraud Survey Report: Identity Fraud Is Dropping, Continued Vigilance Necessary* ("2007 Javelin Survey") (Javelin Strategy & Research, Feb 2007).

[18] Id at 1.

[19] Id.

[20] *Total Number of Fraud Complaints & Amount Paid: Calendar Years 2004 through 2006*, ConsumerSentinel (Feb 7, 2007), online at http://www.consumer.gov/sentinel/Sentinel_CY_2006/total_fraudcomplaints_amountpaid.pdf (visited Jan 12, 2008). For discussion, see also Joseph Pereira, *Bill Would Punish Retailers for Leaks of Personal Data*, Wall St J B1 (Feb 22, 2007) (reporting on a proposed Massachusetts statute that would require retailers to pay for losses when hackers and thieves breach their security systems).

losses of a similar amount. Issuer fraud losses on the Visa system, for example, have hovered around six basis points of volume (0.06 percent) for several years.[21] With volume in 2006 of approximately $1.75 trillion, this amounts to an additional $1 billion.[22] The other major payment card systems report similar amounts of fraud losses. Of course, these figures do not reflect the costs of countermeasures.[23] But even if the cost of fraud is the "modest" $3 billion, it amounts to a real tax on commerce with no offsetting benefits. Javelin's astounding $49.3 billion only raises the stakes.

It seems clear, moreover, that the costs of fraud and fraud prevention are closely related, for any increase in the level of fraudulent activity will quickly transform itself into an increase in the efforts at loss prevention. But that generality conceals a host of other issues, for it does not indicate exactly what duties should be parceled out to whom, or what sanctions should be imposed for their nonperformance. It is on these questions of system design and *marginal* deterrence that we find that the greatest gains come from private ordering.

IV. A MANY-SIDED TRADEOFF

Part of the difficulty in setting the relevant priorities is that the question of fraud prevention cannot be decided in a vacuum. In dealing with payment card risks, it turns out that everyone wants two competing items that they cannot have in an unalloyed form: convenience and security.

The desire for the first of these is evident. We all want payment card transactions to be fast and easy. Speed matters, even when it is measured in terms of seconds. Credit card transactions are not relationship transactions that depend on some element of personal trust. Rather, these are the quintessential impersonal transactions in which all that is desired is prompt and flawless execution—swipe the card, approve the transaction amount, wait for authorization, sign the receipt, go. The more rapid speed makes it possible to use credit cards for transactions in ever smaller dollar amounts. There is, for example, a real effort to reduce the need for signed receipts by using simple swipe transactions. Right now many merchants dispense with signa-

[21] See, for example, Visa USA, Inc, *Quarterly Performance Data Fourth Quarter 2006*, online at http://www.usa.visa.com/download/about_visa/press_resources/statistics/Q42006.pdf (visited Oct 2, 2007).

[22] See id (providing data on total volume for 2006 and the percentage of net fraud).

[23] In 2005, for example, Visa estimated that it was planning to increase spending to combat fraud by $200 million over the following four years. Visa USA, Inc, *Visa USA Annual Report 2005* 1–2, online at http://usa.visa.com/download/about_visa/annual_report.pdf (visited Oct 2, 2007) (discussing challenges from and responses to fraud for Visa).

tures for purchases under $25 in order to keep the lines moving.[24] That premium on speed also opens new markets for credit cards. One instance is their use in parking meters, where the amount of money involved is often under one dollar. Advantages accrue to the consumer, including the ability to choose the exact amount of time to park and the ability to execute a transaction when there is no change jingling in the pocket. For the municipal authority, the use of cards allows for faster collection of funds, and, as a bonus, it eliminates the risk that thieves will break into parking meters.

The desire for convenience necessarily conflicts with the desire for security. Transactions would be more secure if consumers were required to use a form of two-factor authentication to initiate every transaction. But adding a step to a payment card transaction is a bit like putting a pebble in the shoe of a marathon runner; the user winces with every step. Convenience, of course, goes beyond speed. Since mail and telephone order merchants first began accepting payment cards in 1970s, card-not-present transactions have generated a disproportionate amount of fraud. Payment card systems could reduce fraud simply by forbidding people from using them on the internet, over the phone, or through the mail. Doing so, however, would rob payment cards of much of their utility for consumers as well as merchants.

Further complicating matters is the desire for anonymity or, as it is more often described, privacy. We have all engaged in transactions that we want to keep concealed, in whole or part, from some other interested or potentially interested party, as is often the case with pornography and gambling—where billing information often goes out under innocuous descriptions. But anonymity presents a real problem for many transactions, including all payment card transactions. Although a typical payment card transaction may appear to be a simultaneous exchange, it is not. The consumer leaves the store with merchandise, but the merchant merely receives in exchange a promise of payment that must be processed through several layers of intermediaries. In a typical face-to-face transaction, if the merchant has followed the necessary steps, this promise to pay will be supported by a guarantee backed first by the merchant's bank, then by the cardholder's bank, and ultimately by the system itself. Even with a guarantee, however, a promise to pay is not the same as being paid, and there

[24] Visa dispensed with the signature authorization requirement to expand acceptance of its cards at quick service restaurants such as McDonald's and Taco Bell. Typically, quick service restaurants needed to capture signatures at the point of sale in order to avoid liability for fraudulent transactions; a major disadvantage for payment cards relative to cash. Two years ago, however, Visa persuaded issuers to eliminate the requirement and to accept liability for fraudulent transactions, and acceptance in the category has increased dramatically.

is simply no way to enforce a promise against an anonymous counterparty. This brute fact means that someone, somewhere has to keep at least some information about the transaction.

Retaining information needed first to process and then to verify each individual transaction, however, necessarily makes the system less secure. In fact, the more information one party to the transaction feels compelled to retain, the less secure the system becomes. If a merchant that has accepted a payment card retains a complete record of the transaction—including the data on the card that was used to obtain the authorization—its decision presents a real security risk. First off, even if a merchant is beyond reproach, all of its employees may not be. Thus, internal systems have to be devised, similar to those used to protect other trade secrets, to prevent any insider from acquiring the information for illicit purposes. More pressing than the inside threat perhaps, is the outside one: strangers will have a significant incentive to break down the merchant's walls ("hack the system") in order to obtain the information and use it to engage in various forms of identity theft.[25] If the information is valuable enough, an inside/outside combination is always possible. Of course, the information could also be obtained at the original source by stick or trick. "Phishing," after all, is just a new name for the old English crime of larceny by trick, whereby false but suggestive questions or presentations are used to lure people to provide information that allows the trickster to commit fraud.

The 2007 Javelin Survey confirms that securing payment card systems is a multifaceted problem. The problem begins with the source of the information that ultimately gives rise to fraud. In 2007, Javelin asked victims of identity theft if they knew how the information that led to the fraud against them had been taken. Only 42 percent of consumers knew the source. Of those, 75 percent reported that their information was taken directly from them with the remaining 25 percent putting the blame on theft from a third party. Thirty-eight percent of the consumers who knew how their information had been taken identified a lost or stolen wallet, purse, or checkbook as the source of information. "Friendly" fraud—that is, unauthorized use of data by a friend, relative, acquaintance, or in-house employee—and traditional retail sales were the next most reported sources, coming in at 15 percent each. The various sources of cybertheft were identified much less often, and survey responses put two personal sources of cybertheft,

[25] For a vivid description of this market, see Stephen J. Dubner and Steven Levitt, *Identity Crisis*, NY Times Mag 24–25 (Mar 11, 2007) (detailing the ease with which personal identity can be obtained, often in internet chat rooms).

theft of information from a personal computer (8 percent) and phishing (4 percent), ahead of data breaches (3 percent).[26]

The 2007 Javelin Survey does not have much to say about the source of stolen data. When a third party is the source of the stolen information, consumers are unlikely to know the precise source of a breach. Information collected by the Privacy Rights Clearinghouse and analyzed by Richard J. Sullivan of the Kansas City Federal Reserve helps to fill in this gap.[27] Sullivan has sorted the Privacy Rights Clearinghouse data by source of breach and then tabulated the number of incidents and the number of data records exposed. His analysis shows that breaches occur in all segments of the economy—banks and financial services, processors of financial information, health care, retailers, education, and all levels of the government.[28] According to his analysis, breaches have occurred most often, almost 50 percent of the time, in the government and education sectors, but the most records have been stolen from retailers and processors of financial data.[29]

The difficulties of securing payment card systems are compounded by the ways in which thieves can combine information to commit various types of fraud. The information that resides on a payment card is, as discussed above, inherently valuable. A reasonably sophisticated thief can use the stolen data to create counterfeit cards or otherwise generate fraudulent transactions. But payment card information can be combined with other information to commit more elaborate types of fraud. Add in account data and personal identifying information—particularly social security number and mother's maiden name—and the thief can take over an account. By changing an account address and redirecting statements, the thief can both circumvent certain security measures and conceal fraudulent transactions from the true owner. A thief can also use personal information to commit new account fraud—that is, open an account in another person's name. Existing account fraud, which includes classic payment card fraud

[26] 2007 Javelin Survey at 30 (cited in note 17).

[27] See generally Richard J. Sullivan, *Risk Management and Nonbank Participation in the U.S. Retail Payments System*, 92(2) Economic Review 5 (2007).

[28] Id at 15 table 2 (providing percentages of publicly reported data breaches across sectors of the economy).

[29] Id (reporting 19.9 percent and 22.6 percent of all breaches for retail and education respectively and 61,288,322 and 40,691,306 records compromised for retail and processors of financial data respectively compared with, for example, 6,352,711 records compromised for education).

and account takeovers, happens more frequently and generates more total losses. New account fraud is more costly on a per event basis.[30]

V. COMBATING THE PROBLEM ON ALL SIDES

By this point, it should be clear that there is no single solution to combating fraud. At all times, payment card systems must keep their eyes on many balls. In practice, reducing fraud means placing many discrete bets while trying to preserve the attributes that make the systems relatively more attractive than paper-based forms of payment.

Efforts to combat fraud begin with the cards themselves. All of the major card networks, taking a cue from efforts to reduce counterfeiting of paper- and coin- based value exchange systems, have designed their cards to make them more difficult to counterfeit. Holograms, microprinting, and special plastics make the cards difficult to mimic. Card systems also place data in different places on the card to complicate potential fraud schemes. In order to use a card over the internet, for example, a consumer must generally provide the name on the card, the account number, the expiration date and the card security code (the three or four digit number on the back or front of the card that is not part of the primary account number). Although the name, expiration date and account number are generally embossed on the front of the card and readable from the magnetic stripe, the card security code is *only* printed on the card.

Card systems have built elaborate systems to detect fraud as cards are used. In 2005, Visa announced the launch of an advanced authorization system, which looks at card use along two primary dimensions. It compares the new use of a particular card to the historic use of that card, looking for variations that suggest possible fraud. Variations can arise in terms of dollar volume (a low dollar transaction followed by a series of high dollar transactions), geography (a transaction at a merchant in Chicago followed immediately by a transaction in Paris), or merchant type (a series of transactions at online merchants). Visa's system also compares use of one card to use of other cards at or about the same time, again looking for unusual usage patterns.[31]

The systems also set rules for their participants. One key standards organization that addresses these issues is the PCI Security

[30] 2007 Javelin Survey at 5 (cited in note 17) (explaining that the average victim of an existing account fraud paid $587 out of pocket in consumer costs, but if the thief opened a new account in the victim's name, the average consumer had to pay $792).

[31] See *Visa Reaches Major Technology Milestones—Paves the Way for Global Growth and Innovation*, Bus Wire (Sept 27, 2006) (reprinting the VISA press release).

Standards Council[32] (PCISSC), whose mission is "to enhance payment account security" by adopting a set of common practices across the industry.[33] The founding members of PCISSC include all the major credit card companies (whose cooperative action in these matters should, one hopes, be immune from examination under the antitrust laws given the absence of any anticompetitive effects). The recommended procedures involve the creation of secure networks to protect credit card information, to test the networks so created, and to update their design and organization in light of new information about various technical developments and breach. The basic requirements focus among other things on the issue identified above—retention of information. In this case, less is really more, and a good portion of the PCI standard is devoted to identifying the precise data that parties to payment card transactions need to retain to enforce their contracts and telling them what they are able to discard. Beyond that, the requirements discuss the usual litany of efforts to implement system security, including firewall separation, specialized passwords, encryption devices, virus protection, restricted access, unique person IDs, and accessing monitoring and testing devices, all of which seem related to the tasks at hand.[34]

PCISSC—in part for antitrust concerns—is an umbrella group only. It does not impose any specific sanctions on noncompliant businesses. This job falls on the payment card networks themselves. A quick look at the various publications indicate that payment card companies have not been indifferent to this source of loss (as well as to other attacks, such as denial of service campaigns that could be organized by disgruntled employees).[35] The basic program comes in two parts, the first of which requires cooperation for the particular breach. The steps here include immediate reporting to all connected parties, the preservation of all forms of evidence, increased alert, isolation of compromised systems, the filing of reports, and the conduct of general investigations. The second part includes continued demonstrations of compliance with the overall security standards going forward, which relates back to the PCI standards noted above. The consequence of a

[32] See PCI Security Standards Council, *About the PCI Data Security Standard (PCI DSS)*, online at https://www.pcisecuritystandards.org/tech/index.htm (visited Jan 12, 2008).

[33] See PCISSC, *PCI Security Standards Council Appoints Robert M. Russo, Sr. as General Manager* (Mar 27, 2007), online at https://www.pcisecuritystandards.org/pdfs/03-27-07.pdf (visited Jan 12, 2008).

[34] See *About the PCI Data Security Standard (PCI DSS)* (cited in note 32).

[35] See, for example, Visa USA, Inc, *What to Do if Comprised: Visa USA Fraud Investigations and Incident Management Procedures* 1, online at http://usa.visa.com/download/merchants/cisp_what_to_do_if_compromised.pdf (visited Jan 12, 2008).

breach is the imposition of fines and penalties, coupled with the possible termination of business relationships.

The punishments are not trivial in the event of noncompliance. For example, whenever a Visa member fails to immediately notify Visa USA Fraud Control of the suspected or confirmed loss or theft of any Visa transaction information, Visa reserves the right to subject them to penalties of up to $100,000 per incident. Visa may impose fines of up to $500,000 per incident on any compromised merchant or service provider who is not compliant at the time of the incident.[36] In addition, Visa pairs the stick with the carrot, by announcing its willingness to reward compliant firms up to $20 million in incentives while punishing noncompliance: "Specifically for PCI compliance, acquirers will be fined between $5,000 and $25,000 a month for each of its Level 1 and 2 merchants who have not validated by September 30, 2007 and December 31, 2007 respectively."[37] In fact, Visa levied $3.4 million in fines in 2005 and $4.6 million in 2006 for noncompliance.[38] There is also an implicit threat of termination for noncompliance, which would be a death knell for data processing firms and a severe blow to retail firms that want to provide their customers with instant access to bank-supplied credit.

VI. No System Is Perfectly Secure

The holders of confidential information play in one sense a losing game against the hackers and phishers. In order for the overall system to be secure each individual unit within it has to be secure. The hackers and phishers will do very well indeed if they can break through the barriers at even one key target, for the information that they acquire there can be used, often most effectively, against other merchants. The law of large numbers therefore guarantees that some major security breakdowns are likely to happen, even if proper precautions are taken—and almost sure to happen if they are not.

And so the chickens come home to roost. On December 18, 2006, TJX Co—the world's "leading off-price retailer of apparel and home

[36] Visa USA, Inc, *Cardholder Information Security Program*, online at http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html?it=l2|/merchants/risk_management/cis_overview.html|If%20Compromised (visited Jan 12, 2008).

[37] Visa USA, Inc, *Visa USA Pledges $20 Million in Incentives to Protect Cardholder Data* (Dec 12, 2006), online at http://corporate.visa.com/md/nr/press667.jsp (visited Jan 12, 2008). MasterCard's website only offers this cryptic warning: "If a merchant does not meet the applicable compliance requirements of the SDP Program, then MasterCard may levy a noncompliance assessment on the responsible MasterCard member." MasterCard Worldwide, *Compliance Considerations*, online at http://www.mastercard.com/us/sdp/merchants/compliance_considerations.html (visited Jan 12, 2008).

[38] Visa USA, Inc, *Visa USA Pledges $20 Million* (cited in note 37).

fashions"[39]—detected "suspicious software" on its computer system. Three days later, after internal investigation, TJX learned that its computer system had been breached. In mid-January 2007, TJX announced the fact of the breach to the world. In March, TJX revealed publicly that the data breach detected during the height of the 2006 Christmas shopping was the largest known data breach in history.[40]

The breach apparently began in July 2005. A group of thieves, possibly with connections to well-known groups of Romanian hackers and Russian mafia syndicates, pulled into a parking lot outside a Marshalls discount clothing store (a TJX subsidiary) in St. Paul, Minnesota. From the parking lot, they intercepted data that Marshalls was transmitting across a wireless network within the store.[41] They used the data to penetrate at least two nodes on the TJX network—one in the United States and one in Europe. *The Wall Street Journal* concluded that the theft "was as easy as breaking into a house through a side window that was wide open."[42]

The thieves stole a staggering amount of payment card transaction data through this side window. For all transactions between December 31, 2002, and September 2, 2003, TJX had stored "all card data" scanned from the magnetic strip on payment cards without encryption.[43] The payment card industry often describes such data as "track 2" data, and with diligence the information can be used to create counterfeit cards that contain precisely the same data, in exactly the same form as legitimately issued cards.[44] In 2005, thieves apparently took card data for 36,200,000 cards, of which 11,200,000 were still valid at the time of the theft. When TJX began masking the data it stored on its system, the thieves changed their tack, using a program called a "sniffer" to capture this information during the card authorization process. As TJX's Form 10-K explains, "the technology utilized in the Computer Intrusion during 2006 could have enabled the Intruder to steal payment card data . . . during the payment card issuer's

[39] The TJX Companies, Inc, Form 10-K for the Year Ending January 27, 2007 at 2, 7 (providing a brief discussion of the company's market position and information about the computer intrusion).

[40] Joseph Pereira, *Breaking the Code: How Credit-Card Data Went Out Wireless Door—In Biggest Known Theft, Retailer's Weak Security Lost Millions of Numbers*, Wall St J A1 (May 4, 2007).

[41] Id (describing the methods and technology by which the information was intercepted).

[42] Id (quoting a source identified as a "person familiar with TJX's internal probe").

[43] See TJX Companies, Inc, Form 10-K at 9 (cited in note 39) (indicating that the "security data included in the magnetic stripe on payment cards required for card present transactions ('track 2' data)" was no longer stored on the system *after* September 2, 2003).

[44] See Larry Greenemeier, *TJX Stored Customer Data, Violated Visa Payment Rules*, Info Week (Jan 29, 2007), online at http://www.informationweek.com/story/showArticle.jhtml?articleID=197001447 (visited Jan 12, 2008) (criticizing the length for which TJX stored its customer data and detailing how information is intercepted).

approval process, in which data (including the track 2 data) is transmitted . . . without encryption."[45]

The thieves found other information on the TJX system as well. Until TJX detected the intrusion on its system, it collected and stored personal information about customers who returned merchandise without a receipt as well as information about at least some customers who paid for their purchases with checks. This personal information included "drivers' license, military and state identification numbers (referred to as 'personal ID numbers'), together with related names and addresses."[46] Moreover, in at least some cases, the personal ID numbers collected by TJX "were the same as the customers' social security numbers."[47] For transactions that took place prior to April 7, 2004, TJX held this data in unencrypted form. TJX specifically identified 451,000 customers whose personal information (as opposed to payment card information) it had exposed to the data thieves, though the actual number may have been far higher.

Data stolen from TJX was apparently put to use before TJX learned of the breach. In March 2007, police in Florida arrested part of a ring of people who had committed fraud using data previously stolen from TJX.[48] The members of the ring apparently created counterfeit cards with the TJX data. They then used the counterfeit cards to purchase stored value cards.[49] The members of the ring then spent the money stored on the stored value cards at various merchants. All told, the members of the ring bought $8 million worth of merchandise at various Wal-Mart stores in Florida.[50] Fraudulent transactions in Georgia, Louisiana, Sweden, and Hong Kong have also been linked to the TJX breach.[51] According to at least one published report, Florida police had told TJX in November 2006 that a gang in Florida was using information stolen from the TJX computer system to create counterfeit cards.[52]

[45] TJX Companies, Form 10-K at 9 (cited in note 39).

[46] Id at 8.

[47] Id.

[48] See Jaclyn Giovis, *6 Held in Credit ID Theft Case; Authorities Link S. Florida Suspects to TJX Cos. Breach*, Ft Lauderdale Sun-Sentinel 1D (Mar 24, 2007).

[49] A stored value card looks like a typical general purpose payment card, but instead of accessing a credit limit or a checking account, it accesses an electronic purse.

[50] Evan Schuman, *Stolen TJX Data Used in $8M Scheme before Breach Discovery*, eWeek.com (Mar 21, 2007), online at http://www.eweek.com/article2/0,1895,2106149,00.asp (visited Jan 12, 2008).

[51] Matt Hines, *Data from TJX Security Breach Fuels Fraud Scheme*, CSO (Mar 21, 2007), online at http://www2.csoonline.com/blog_view.html?CID=32617 (visited Jan 12, 2008).

[52] Id.

VII. THE AFTERMATH

The immediate question in the wake of the TJX breach is who bears the cost. As it turns out, this is not as simple a question as it might seem. The costs associated with a breach come in two forms—fraud that arises from the use of the stolen data and efforts to reduce such fraud. In the first instance, neither set of costs falls on TJX. When payment card data is stolen from one merchant and used fraudulently at another merchant, the fraud losses fall on either the bank that issued the card or the merchant at which the stolen information was used. The costs of efforts to mitigate such losses likewise fall on issuers and other merchants. This initial distribution is not fixed. Each of the major electronic payment systems administers a dispute resolution process that redistributes the costs associated with a breach of the sort experienced by TJX. Although one would expect participants in these systems to settle on the optimal distribution of cost, the matter has not been left to private contract.

Some efforts to redistribute losses have been foreclosed by federal law. As we noted earlier, the 2007 Javelin Survey identifies lost or stolen cards and "friendly" fraud as the first and second most common sources of stolen information. Although the individual losses from such events are small when compared with a large system breach, in the aggregate, such losses add up. One might think then that issuers and systems would put some of the onus for fighting fraud on consumers. If a consumer were subject to the risk for potential losses arising from unauthorized use of a stolen card, one would expect the consumer to raise the issue with the issuing financial institution rather promptly. At present, however, federal law limits the liability of credit card holders to $50 per card, no questions asked.[53] We 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.

As it turns out, the federal standard has relatively little bite. Market pressures have pushed the balance still further, insulating payment card users from essentially all fraud losses. Visa, for example, advertises a "zero liability" policy on its website.[54] We think that two reinforcing trends explain this result. First, the customer whose card is stolen suffers even if he pays nothing in cash, if only from the major inconvenience of the disruption of service which could (if the losses

[53] 15 USC § 1643(a)(1)(B) (2000).

[54] See Visa USA, Inc, *Visa Security Program*, online at http://usa.visa.com/personal/security/visa_security_program/zero_liability.html (visited Jan 12, 2008).

persist) lead to a refusal to maintain the account. Therefore, no individual liability should not be confused with no individual loss. Second, the improved systems of detection, plus the background level of customer cooperation (even in the absence of liability), are sufficient to explain the strong market trend away from any form of customer liability (which should give some pause to those who think that preemptive consumer protection laws "improve" upon market outcomes).

Consumers are not the only participants who object to bearing a share of the costs associated with system security. Other parties have also looked for relief outside the system. Just three months after the TJX breach became public, several small financial institutions, joined by a handful of associations of such institutions, filed a class action lawsuit against TJX in the United States District Court for the District of Massachusetts. They claimed that TJX had violated state and federal laws relating to negligent misrepresentation, unfair and deceptive acts, and negligence in the retention and control of these databases in addition to breach of contract claims.[55] The relief sought included compensation for the reissued cards and all fraudulent transactions traced to the breach.[56] The complaint is drafted under the rules of notice pleading so it gives little indication of how the various causes of action interact with each other, and we are inclined to think that virtually all the counts here are duplicative of the breach of contract action. Thus count one, dealing with negligent misrepresentation, only asserts that the defendant "falsely represented that it would comply with" the various Card Operating Regulations, which adds little to the point that they did not so comply.[57] The use of the ostensible tort action is probably meant to operate as an end run on limitations on damages in the contract claim, and we see no reason why it should be the source of any additional relief.

In this regard, the litigation in the wake of the TJX breach has followed the path of litigation in the wake of previous security breaches. After the discovery of the breach at BJ's Wholesale Club, a number of financial institutions filed claims for fraud losses and reissuance costs.[58] They alleged contract, tort, and consumer protection claims against BJ's and its merchant bank, Fifth Third. The district court dismissed all the contract claims except the contract claim

[55] Class Action Complaint, *In re TJX Companies Retail Security Breach Litigation*, No 07-10162 ¶ 3 (D Mass filed Apr 25, 2007).

[56] Id ¶¶ 72–74.

[57] Id ¶ 81.

[58] See, for example, *Pennsylvania State Employees Credit Union v Fifth Third Bank*, 398 F Supp 2d 317, 322–23 (MD Pa 2005).

against Fifth Third[59] and concluded that the plaintiffs had stated a claim against Fifth Third as third-party beneficiaries of the contract—the Operating Regulations—between Visa and Fifth Third.[60] It dismissed a parallel claim against BJ's, noting that the plaintiffs had not (and could not) allege a direct contractual relationship between Visa and BJ's and that the contract between Fifth Third and BJ's specifically disclaimed any obligation to third parties. Ultimately, the third-party beneficiary claim against Visa failed because Visa intended its rules to benefit the system as a whole as opposed to any specific issuer.[61]

Financial institutions have had considerably more success shifting costs through state legislatures. In the immediate wake of the TJX breach, Minnesota adopted a law that prohibits merchants accepting card payment from retaining certain information. Like the PCI standard, the Minnesota law forbids merchants from retaining the contents of the magnetic stripe.[62] Minnesota law also makes a merchant responsible for whomever it hires to process payment card transactions, imputing to the merchant the service provider's retention of information. The kicker comes in the assessment of damages: parties (read: merchants) that violate the Act are held, in essence, fully liable for all consequential damages sustained by banks in canceling or reissuing credit cards, closing accounts or otherwise managing their usual business, and any refund or credit that must be issued to a bank customer.

We do not profess to have any divine knowledge as to whether these various transfer payments from retailers to banks make good sense as a matter of policy. But we are equally confident that the Minnesota legislature has no better information on this point than we have. Minnesota's response to the TJX breach suffers from several obvious problems:

- First, payment cards operate on national networks, which suggests the need for a uniform, presumably federal, rule for all financial institutions and merchants. Fifty different state regimes will create havoc for merchants, networks, financial institutions, and, ultimately, consumers.

[59] Id at 338.

[60] Id at 332–37.

[61] See *Pennsylvania State Employees Credit Union v Fifth Third Bank*, 2006 WL 1724574, *1 (MD Pa) (memorandum opinion). See also *Cumis Insurance Society, Inc v BJ's Wholesale Club, Inc*, Civil Action No 05-1158, *2 (Mass Super Ct filed Dec 1, 2005) (memorandum opinion) (rejecting a similar claim in Massachusetts).

[62] See Act of May 21, 2007, 2007 Minn Laws 108, to be codified at Minn Stat Ann § 325E.64 (West 2007) (mandating a forty-eight hour limit on the retention of personal information following a transaction).

- Second, however sensible the liability standard seems today, it will quickly become outdated. As noted above, payment card systems and fraudsters are engaged in a constant struggle, and fraud prevention efforts that seem state of the art today (for example, imposing a forty-eight hour limit on retention of card data) will very quickly become outmoded.
- Third, the statute fails to recognize how its liability and damage provisions relate to all of the other provisions of the elaborate contracts that currently bind participants in the payment card networks. In particular, the statute completely fails to recognize the fact that the shift in the liability rules may increase the costs of payment card acceptance to merchants to the point that they either drop out of the systems entirely or demand some reduction in the fees that they pay.
- Fourth, the statute awards unliquidated damages to injured financial institutions. We recognize that modern rules of damages typically award unliquidated damages even in commercial disputes. Nevertheless, we note that nearly all well-drawn commercial agreements rule out consequential damages determined on a case-by-case basis in favor of a liquidated damages standard.

In sum, the new legislation will add a new layer of cost and uncertainty to the payment card system. The new statute appears to favor card issuers over retailers and processors. But in the long run, that state of affairs cannot last. Merchants do not, after all, have to accept payment cards sponsored by Visa and MasterCard in order to stay in business. Although payment cards offer many advantages over other forms of payment, particularly cash and checks, there are limits to the price that merchants will pay and the risks that they are willing to bear. Legislation of the sort adopted in Minnesota may have the effect of pushing merchants to adopt other forms of payment that do not pose some of the risks presented by payment cards. This legislation is likely to introduce serious distortions, first because of its high administrative costs, and second because of its unintended incentives on the relevant parties.

To say so does not deny public authorities a role in combating payment fraud on payment card networks. By imposing criminal sanctions on data thieves and investing resources in efforts to prosecute theft of payment card data, public authorities no doubt reduce the total amount of fraud. However, this role does not extend to preempting efforts on the part of private actors to distribute losses that arise from such breach. Unfortunately, the leap from step one to step two is all too frequent. Perhaps the most prominent recent instance of this cycle is the passage of the Sarbanes-Oxley Act[63] in response to the corporate scandals that took place at Enron, WorldCom, and the like. The mistake that doomed the governmental response is operative in this case: the deep legislative conviction that they know more about the optimal contracting strategies for risk allocation than the immediate, and sophisticated, parties to the transaction. In Sarbanes-Oxley, this worldview led to stringent conditions on independent directors and auditing requirements, which encumber well-run firms as well as poorly run ones.[64] The upshot is a change in corporate culture, a loss of initial public offerings to Europe and Asia, and a robust "going private" movement. We do not think that efforts to legislate responses to credit card fraud are likely to have the dramatic consequences of Sarbanes-Oxley, but not for want of trying.

[63] Pub L No 107-204, 116 Stat 745 (Supp 2002).

[64] Michael Bloomberg and Charles Schumer, *Sustaining New York's and the US' Global Financial Services Leadership* 19–20, online at http://www.senate.gov/~schumer/SchumerWebsite/pressroom/special_reports/2007/NY_REPORT%20_FINAL.pdf (visited Jan 12, 2008). See generally Roberta Romano, *The Sarbanes-Oxley Act and the Making of Quack Corporate Governance*, 114 Yale L J 1521 (2005) (noting that Sarbanes-Oxley represents a change in regulation regimes, moving from disclosure requirements to substantive corporate governance mandates and arguing that the change resulted from hasty decisionmaking, not careful legislative deliberation).