

CYBERSECURITY IN THE PAYMENT CARD INDUSTRY
BY
RICHARD A. EPSTEIN & THOMAS BROWN

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 that 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 the 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 net entrants.¹ Using a payment card (as opposed to some other form of payment) rests on voluntary decisions by consumers and the 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 makes it highly unlikely that those results could be realized.

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

¹ For our view on the antitrust issue, see Thomas Brown, 73 U. Chi. L. Rev. Richard A. Epstein & Thomas Brown, *The War on Plastic*, Regulation 12 (Fall, 2006); Richard A. Epstein, *Behavioral Economics: Human Errors and Market Corrections*, 73 U. Chi. L. Rev. 111 (2006); *The Regulation of Interchange Fees: Australian Fine-Tuning Gone Awry*, 2005 Colum Bus L Rev 551. On the new entry front, the last several years have witnessed the emergence of companies trying to take on the primary incumbents—American Express, Discover, MasterCard, Star and Visa. Steve Case has backed a new credit card network known as the Gratis card. [cite]. A group of merchants have teamed up to launch a debit card network known as Tempo. [cite]. eBay’s PayPal and Pay-By-Touch also compete with the more established payment network at least to the extent that they enable consumers to initiate debit transactions that clear over the ACH networks rather than the networks sponsored by the established players. [cite]

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

ceases, without undertaking the hard work to find what contractual and institutional arrangements work best to combat the fraud that everyone deplures. If fraud is bad, then what mix of public and private systems should be used to implement a coherent policy of fraud prevention that arises in connection with 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?

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.

A QUICK TOUR OF THE LAW OF THEFT 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 to include any knowingly unauthorized use of a thing by a bailee or other servant who took possession from the owner.³ The penalties for theft were harsh, calling initially for death and later for severe penalties.⁴ 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 knowledge of the theft.⁵ The obvious point for this regime was to reduce the incentive for theft by reducing the gains that the thief could obtain by scaring off potential buyers, when the value of the property stolen was greater in sale than in use, as frequently happens with stolen goods.

For its part the early English law on 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.⁶ 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

³ For the relevant materials, see Gaius Institutes, III, 195-197; for a general discussion, see Barry Nicholas, *Introduction to Roman Law* (1962). We are aware of, but do not discuss, the legal refinements that address such questions of whether a servant or customer is in possession of an object or only has mere custody of it. See, e.g., *The Case of the Carrier Who Broke Bulk Anon v. The Sheriff of London*, YB Pasch. 13 Edw. IV., f. 9, pl. 5 (1473), 64 Seldon Soc. 30 (1945).

⁴ Gaius, at III, 189.

⁵ *Id.* at III, 186-187.

⁶ For an exposition see, George P. Fletcher, *The Metamorphosis of Larceny*, Harv. L. Rev.

embezzlement—had to be grafted onto this paradigm case to close the gap.⁷ In more modern times, as information becomes 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,⁸ 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 calls for criminal penalties, including fines, imprisonment, and forfeiture.⁹ The federal statute also extends its prohibitions to anyone who “receives, buys, or possesses,” such information.¹⁰

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 theft 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 various forms of theft. The usual rule starts with the simple proposition that in the first instance the loss from theft falls directly 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 fall short, private individuals will take precautions that start with door and progress to elaborate security systems designed to guard against the 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 steps for self-protection. It is therefore difficult in the abstract to judge the relative effectiveness of the two systems in preventing loss. The plot, moreover, 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 number of individuals in ordinary cases, as is necessarily the case with routine credit information.

⁷ For the variations, see Model Penal Code, Article 223, especially, Section 223.1(1) calling for the consolidation of theft offenses.

⁸ *Id.* § 223.0(6) (definition of property).

⁹ Economic Espionage Act of 1996, 18 U.S.C. § 1831-1839, with broad coverage with respect to conversion of trade secrets “related to or included in a product that is produced for or placed in interstate or foreign commerce,” *Id.* at § 1832, which covers just about every commercial secret. Fines and imprisonment are cover in § 1832(a). Criminal forfeiture is covered in § 1834.

¹⁰ *Id.* § 1832(a)(3).

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.¹¹ 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 transaction was not large enough to warrant any revision of the initial loss provisions. But in all settings, the debates were only instrumental, 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 generate an expected reduction of one dollar in the value of the property stolen—a standard that is hard to implement in practice, when there are so many moving margins at any one time.

The Two-Tiers in Payment Card Markets We think that this basic two part program carries over without a beat to the various financial losses that are associated with payment card transactions. There is little doubt today that extensive criminal sanctions are properly imposed on persons who steal valuable payment card information. But prosecuting these thefts is often perilous business. The thefts, as we shall see, are often made surreptitiously and at a distance. Their clever nature 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, 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. Stolen payment card information is worthless to the thief unless it can be used to generate a transaction. In order to be used,

¹¹ For the Roman rules, see Gaius Institutes, III, 203-208.

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—*e.g.*, 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? The structure of the typical credit card transaction 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 in the chain 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. 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 from themselves.¹² 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.¹³ Javelin estimated that total fraud in 2007 from identity theft was \$49.3 billion.¹⁴ This astounding number actually represents a decline from previous levels. In 2003, Javelin estimated that total fraud resulting from identity theft was \$53.8 billion.¹⁵ Although Javelin's definition of fraud may overstate the actual losses from fraud, other sources confirm that the actual costs of fraud are significant. According to the FTC, consumers

¹² For a similar view about cybersecurity issues more generally, see Robert W. Hahn and Anne Layne-Farrar, *The Law and Economics of Software Security*, 283, 286 (2006), on the unexceptionable ground that the cure is often worse than the disease.

¹³ For latest version, see Javelin Strategy & Research, *2007 Identity Fraud Survey Report: Identity Fraud Is Dropping, Continued Vigilance Necessary* 1 (2007).

¹⁴ *Id.* [Javelin 2007]

¹⁵ *Id.* [Javelin 2007]

reported credit card fraud losses of \$1.2 billion in 2006, up significantly from 2005.¹⁶ Financial institutions report fraud losses of a similar amount. Issuer fraud losses on the Visa system, for example, have hovered around 6 basis points of volume (.06%) for several years.¹⁷ With volume in 2006 of approximately \$1.5 trillion, this amounts to an additional \$750 million.¹⁸ The other major payment card systems report similar amounts of fraud losses. Of course, these figures do not reflect the costs of countermeasures.¹⁹ But whether the cost of fraud is \$3 billion or Javelin's astounding \$49.3 billion, it amounts to a real tax on commerce with no offsetting benefits.

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.

A Many-Sided Trade-Off Part of the difficulty in setting the relevant priorities is that the question of fraud prevention cannot be decided in a vacuum. There is a full range of considerations that must be taken into account to set matters right. In dealing with payment card risks it turns out that everyone wants two competing items which 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.²⁰ The more rapid speed makes it possible to use credit cards for transactions in ever smaller 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 signatures for purchases under \$25 in order to keep the lines moving. That premium on speed also opens new markets for credit cards. One instance is their use in parking meters, where the amount of money

¹⁶ For discussion see Joseph Pereira, *Bill Would Punish retailers for Leaks of Personal Data*, Wall Street Journal February 22, 2007.

¹⁷ [Confirm/Nilson Report?]

¹⁸ [confirm/Nilson Report?]

¹⁹ 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 2005 Annual Report].

²⁰ And even the signing is now dispensed with in some outlets where the purchase is for \$25 or less.

involved is often under \$1.00. 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 things 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 the 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 is simply no way to enforce a promise against an anonymous counterparty.²¹ This brute fact means that someone, somewhere has to keep at least some information about the transaction.

But retaining information needed first to process and then to verify each individual transaction 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—this present a real security risk. First off, even if merchant itself is

²¹ Howard Beales, Associate Professor of Strategic Management and Public Policy at George Washington University and former Director of the Bureau of Consumer Protection at the Federal Trade Commission, has described the desire for a mechanism that would enable perfect enforcement of anonymous contracts as yet another version of the “Nirvana fallacy,” whereby we compare the imperfect institutions we have with the perfect ones that we are all capable of imagining.

beyond reproach, all of its employees may not be, so that 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 means. More pressing than the inside threat perhaps, is the outside one: strangers will have a significant incentive to break down the merchant's walls (*i.e.*, "hack the system") in order to obtain the information and use it to engage in various forms of identity theft.²² 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% of consumers knew the source. Of those, 75% reported that their information was taken directly from them with the remaining 25% putting the blame on someone with which they did business. Thirty-eight percent of the consumers who knew how their information had been taken identified a lost or stolen wallet, purse or check book as the source of information. "Friendly" fraud—*i.e.*, 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%. The various sources of cybertheft were identified much less often, and survey responses put two personal sources of cybertheft, theft of information from a personal computer (8%) and phishing (4%), ahead of merchant data breaches (3%).²³

The difficulties are compounded by variety in the type of fraud. Payment card fraud falls into two major categories, fraud on existing accounts and new account fraud. Existing account fraud generally takes one of two basic forms. In the classic payment card fraud, the fraudster runs up unauthorized transactions until detected by the real cardholder or the issuing bank. Account takeover represents a more sophisticated scheme. With an account takeover, a fraudster uses other personal information gathered about a cardholder to gain effective control of an account, *e.g.*, changing the address to which statements are sent and, in some cases, asking for new plastics to be issued. When a fraudster takes control of an account, he can present himself as the rightful owner of the account to the rest of the world. New account fraud works a bit like an account takeover. The fraudster uses personal information about another person to open accounts in that person's name, running up charges until detected either by the rightful owner of the identity or the issuing institution. Of the two types of fraud, existing account fraud

²² For a vivid description of this market, see Stephen J. Dubner and Steven Levitt, *Identify Crisis*, *New York Times*, March 11, 2007

²³ Javelin, 2007 Identity Fraud Report at 30.

accounts for more total dollars of fraud, but new account fraud is more costly on a per event basis.²⁴

Combating The Problem On All Sides By this point, it should be clear that there is no single solution to combating fraud. In order to combat fraud, 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. They use holograms, microprinting and special plastics to make the cards difficult to mimic. They include additional data on a card that fraudsters must collect in order to use the cards. 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 (*i.e.*, the three or four digit number on the back or front of the card that is not part of the primary account number).

They have also built elaborate systems to detect fraud as cards are used. In 2005, Visa announced the launch of an advance authorization system. Visa's system 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 (*i.e.*, a low dollar transaction followed by a series of high dollar transactions), geography (*i.e.*, a transaction at a merchant in Chicago followed immediately by a transaction in Paris) or merchant type (*i.e.*, a series of transactions at on-line 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.

The systems also set rules for their participants. One key *standards* organization that addresses these issues is the PCI Security Standards Council, whose mission is "to enhance payment account security" by adopting a set of common practices across the industry. 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 effect). 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 *inter alia* 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,

²⁴ *Id.* [Javelin 2007] at 4.

restricted access, unique person IDs, accessing monitoring and testing devices, all of which seem related to the tasks at hand.²⁵

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).²⁶ 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 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.²⁷ In addition, Visa pairs the stick with the carrot, by announcing its willingness to reward complaint firms up \$20 million in incentives while punishing non-compliance: “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.”²⁸ In fact, Visa levied \$3.4 million in fines 2005 and \$4.6 million in 2006

²⁵ See About the PCI Data Security Standard , <https://www.pcisecuritystandards.org/tech/index.htm>.

²⁶ See, e.g., Visa USA, What to Do if Comprised: Fraud Investigations and Incident Management Procedures, available at

²⁷

http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html?it=12|/merchants/risk_management/cisp_overview.html|If%20Compromised

²⁸

http://usa.visa.com/about_visa/press_resources/news/press_releases/nr367.html?it=c|/merchants/risk_management/cisp.html|Read%20Press%20Release. The MasterCard response is less apparent: Their website offers a cryptic: “If a merchant does not meet the applicable compliance requirements of the SDP Program, then MasterCard may levy a non-compliance assessment on the responsible MasterCard member.” http://www.mastercard.com/us/sdp/merchants/compliance_considerations.html

for non-compliance. There is also an implicit threat of termination for non-compliance, 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.

Some fraud prevention efforts, however, have been foreclosed by law. As we noted earlier, the 2007 Javelin survey identifies lost or stolen cards and “friendly” fraud as the first and second largest 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 on the risk for potential losses arising from unauthorized use of a stolen card, one would expect that consumer to raise the issue with the issuing financial institution rather promptly.

In fact, the tendency on this point has run sharply in the opposite direction. At present, federal law places a limit on the liability of credit card holders to \$50 per card, no questions asked.²⁹ We see no reason even for this (modest) restriction on freedom of contract, for if credit card companies thought it was appropriate to impose larger penalties, then, once disclosure is made of the charges, we see no reason why the losses should be socialized as a matter of law. But in fact the federal standard has had relatively little bite, because market pressures have by and large pushed the balance still further, by insulating credit card users from all charges. We think that the explanation for this result lies in two reinforcing trends. 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 persist) lead to a refusal to maintain the account. No liability therefore should not be confused with no loss, for the hassle remains even if credit card companies do (as it is in their interest to) expedite their responses to stolen cards. 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).

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.

²⁹ 15 U.S.C. § 1643(a)(1)(B).

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 fashions”³⁰—detected “suspicious software” on its computer system. Three days later, after internal investigation RIGHT 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.

The breach apparently began in July 2005. A group of thieves, possibly with connections to well-known groups of Romanian hackers and Russian organized crime 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.³¹ They probably used a booster antenna of the sort sold at countless computer stores to capture the data. At the time, TJX had apparently not upgraded security on the wireless network at the Marshalls store in St. Paul. Instead of the more secure Wi-Fi Protected Access standard, TJX was relying on the fairly easy-to-penetrate Wired Equivalent Standard to secure its wireless transmissions. The thieves picked up data that TJX used “to communicate price markdowns and manage inventory,”³² which they used to set-up shop within TJX’s computer network, penetrating at least two nodes on the TJX network—one in the United States and one in Europe. As TJX explained in its 10-K filed with the SEC in March 2007, the data thieves transferred data from the European node to the U.S. node. After discovering the breach, TJX found approximately 100 outside files on its system that it could not decipher.³³ The Wall Street Journal concluded that the theft “was as easy as breaking into a house through a side window that was wide open.”³⁴

The thieves stole a staggering amount of payment card transaction data through this side window, including payment card information for approximately half of all payment card transactions made at TJX stores in the U.S., Puerto Rico and Canada from

³⁰ TJX Co. 10-K at 2 (March 28, 2007) (<http://www.sec.gov/Archives/edgar/data/109198/000095013507001906/b64407tje10vk.htm>)

³¹ Joseph Pereira, *How Credit-Card Data Went Out Wireless Door*, A12 Wall St. J. (May 4, 2007).

³² *Id.*

³³ TJX Co. 10-K at 9 (“Through our investigation, we have identified approximately 100 files that we believe the Intruder, during this period, stole from our Framingham system (the vast majority of which we believe the Intruder created) and that we suspect included customer data. However, due to the technology utilized by the Intruder, we are unable to determine the nature or extent of information included in these files.”).

³⁴ *Id.* (quoting a source identified as a “person familiar with TJX’s internal probe”).

December 31, 2002, through June 28, 2004. For all transactions between from December 31, 2002, and September 2, 2003, TJX had stored “all card data” scanned from the magnetic from the magnetic strip on payment cards without encryption.³⁵ The payment card industry often describes such data as “track 2” data, which means the information can be easily used to create counterfeit cards that contain precisely the same data, in exactly the same form as legitimately issued cards.³⁶ 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 the thieves returned to the TJX system in 2006, they changed their technique. By that time, TJX was masking its stored card account numbers. Instead of retrieving this information from the TJX system, the thieves used a “sniffer” to capture this information during the card authorization process. As the TJX 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 approval process, in which data (including the track 2 data) is transmitted . . . without encryption.”³⁷ The thieves also apparently “had access to the decryption tool” used by TJX—which could easily suggest inside cooperation—to help decrypt other payment card data.

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.” Moreover, in at least some cases, the personal ID numbers collected by TJX “were the same as the customers’ social security numbers.” 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 put to use apparently 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. The members of the ring apparently created counterfeit cards with the TJX data. They then used the counterfeit cards to purchase stored value cards.³⁸ The members of the ring then spent the money stored on the stored

³⁵ See TJX Co. 10-K at 9 (describing the data stored on its system as including “the security data included in the magnetic strip on payment cards for card present transactions).

³⁶ [Cite].

³⁷ TJX Co. 10-K at 9.

³⁸ 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.

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.³⁹ Fraudulent transactions in Georgia, Louisiana, Sweden and Hong Kong have also been linked to the TJX breach.⁴⁰ 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.⁴¹

Losses associated with these and similar counterfeit transactions generally fall, in the first instance, on the either the merchants at which the counterfeit cards were used or the banks that issued those cards. For face-to-face transactions, the risk lies with the issuer that approves the transaction so long as the merchant follows the basic rules associated with authorization. In practice, this means the merchant must be able to present a receipt for the transaction signed by the consumer if the transaction is disputed. For card not present transaction, the merchant generally bears the risk.⁴² In order to mitigate potential losses, a number of financial institutions reissued the cards exposed in the TJX breach.

As one might expect, litigation has also ensued. In April 2007, several associations of small financial institutions and several individual financial 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, and unfair and deceptive acts, negligence in the retention and control of these data bases in addition to breach of contract claims. The relief sought included compensation for the re-issued cards and all fraudulent transactions traced to the breach.⁴³ The complaint is drafted under the rules of notice pleading so it gives little indication of how the various cause 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. The use of the ostensible tort

³⁹ Evan Schuman, *Stolen TJX Data Used in \$8M Scheme Before Breach Discovery* (March 21, 2007) (available at <http://www.eweek.com/article2/0,1895,2106149,00.asp>)

⁴⁰ *Id.* [Hines].

⁴¹ Matt Hines, *Data from TJX Breach Fuels Fraud Scheme* (March 21, 2007) (available at http://www2.csoonline.com/blog_view.html?CID=32617).

⁴² These generalizations oversimplify the rules in at least two ways. First, the networks have slightly different rules for allocating responsibility for different types of transactions. Second, individual networks do not treat all transactions in precisely the same way. Internet merchants that accept Visa, for example, can use the Verified by Visa to shift liability for transactions to issuers. *See also* Levitt/Dubner.

⁴³ Class Action Complaint, *In re TJX Companies Retail Security Breach Litigation*, Master Docket No. 07-10162-WGY (April 25, 2007).

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. Similar arguments apply to the other cases. Quite simply,

Legislative Reforms. At the end of the day, the TJX breakdown prompted the standard response to major breakdowns within the legal system: a call for legislative reform intended to fix the problem. We have no objection to that approach if there were reason to think that the criminal sanctions imposed on the actual thieves were insufficient to the task. But in general we think that there is a strong presumption that the contractual devices should be regarded as the sole source of obligation among the parties, so long as there is a manifest intention to do so. We realize that this leave only a relatively small field for government intervention in the business arrangements, but regard that as a plus. Contract regimes can also be updated in response to new information, through the usual two step process where by the parties cooperatively agree on the optimal set of precautions only thereafter to bargain of payment terms in light of the new level of risks. We are confident that the process will take place, if it has not already, inside the credit card industry.

In general, legislatures do not, however, look solely to the criminal side of matters, but seek to intervene in the contractual domain as well. Perhaps the most prominent recent instance of this cycle is the passage of Sarbanes-Oxley 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.⁴⁴ The statute did not take into account any subtle differences between different types of firms, whether measured by nature of market niche, distribution of shareholder ownership, long-term industry products and the like. The one-size-fit-all approach fit poorly in many firms, and the response was predictable. Some firms sought to scramble in the search for compliance and in the process appointed different types of individuals to boards and committees than might have otherwise been the case. In other cases, the responses were more dramatic. Much of the business in initial public offerings has drifted off to Europe and Asia, the “going private” movement has captured a number of large public firms; and smaller firms are less likely to go public than before. And to top it all off, there is little reason to think that the new systems in place will have a dramatic effect on the frequency and incidence of fraud.⁴⁵

We do not think that any efforts to legislate responses to credit-card fraud are likely to have the dramatic consequences of Sarbanes-Oxley, but not for want of trying. In general, the best way to judge the mischievous effect of legislation is to ask the extent

⁴⁴ Citation

⁴⁵ Citation.

to which it deviates from the contractual norms of experienced players. That gap is likely to be larger with a comprehensive statutory scheme like Sarbanes-Oxley than it is with any fraud prevention legislation. But that said, Sarbanes-Oxley does not set the standard for intelligent legislative reform. Our judgment of the negative expected value of any legislative reform that overrides the contractual arrangements governing these losses seems to be borne out by an examination of legislation adopted in Minnesota, which may yet become a template for national legislation on the same subject.⁴⁶

The stated objective of the Minnesota statute is the protection of payment card data.⁴⁷ As with the PCI standard, the Minnesota law focuses on the retention of information related to payment card transactions:

No person or entity conducting business in Minnesota that accepts an access device [defined to include cards as well as other devices containing the necessary information to initiate a transaction] in connection with a transaction shall retain the security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction.⁴⁸

In addition, the law makes the merchant (*i.e.*, the person accepting the card) responsible for whomever helps it process payment card transactions, imputing to the merchant the service provider's retention of information. The kicker comes in the assessment of damages for parties, typically retailers, that are not found in compliance with the Act, for they 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. In addition, this statute has particular orders on the best way in which to deal with data that retailers acquire in connection with both credit and debit card transactions. It provides that retailers can hold debit card information for at most 48 hours. For credit card transactions, it prohibits the retention of any magnetic strip information after the transaction is completed. It is as if the legislature has proposed minimum standards for burglar alarms in private businesses and homes.

⁴⁶ See Statement of Chairman Barney Frank on the Recent Disclosure of a Major Credit Breach, January 18, 2007. http://www.house.gov/apps/list/press/financial_svcs_dem/pr01182007.shtml. Similar legislation is now been proposed in Massachusetts, House Ho. 213, The Commonwealth of Massachusetts, Chapter 66B. Similar legislation is afoot in California, Connecticut, Illinois and Texas. CITATIONS

⁴⁷ House Ho. 213, The Commonwealth of Massachusetts, Chapter 66B.

⁴⁸ H.F. 1758, <http://www.revisor.leg.state.mn.us/bin/showPDF.php>

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. But we do note several observations about damage regimes in general that should apply to these cases.

First, credit cards operate on national networks, and this seems like an ideal occasion to provide a uniform rule for all banks and consumers. Within the framework, a uniform federal standard seems preferable, and we see no reason why we should have 50 different state regimes. The Minnesota system, moreover, appears to put special burdens on in-state parties for the benefit of financial institutions around the country. There is, moreover, no necessity for other states to follow this pattern. The earlier versions of the Massachusetts law, for example, extended the remedies only with respect to credit cards held by Massachusetts residents. But no matter how the in-state/out-of-state game gets played, it is sure to introduce needless duplication and variation. If there is to be any legislation at all, here is a clear case for a uniform rule of federal preemption.

Second, we are deeply suspicious of any regime that mandates the use unliquidated measures of damages, without any limitation, in commercial disputes. We are fully aware that these tests seem to follow from the modern rules of damages, but at the same time think that it is far more probative of efficient commercial practices to note that virtually all well-drawn commercial agreements rule out consequential damage determined on a case by case basis, and substitute in their place some liquidated sum of damages that bears some relationship to the breach, but which is not calculated exactly.⁴⁹ In this regard, we think that the standard agreements designed by the credit card companies, binding on both banks and retailers, offer a cheaper way to resolve this problem in the cases where some intervention is required. We see no reason to think that this system of public enforcement will do better than the private system that it displaces. Nor do we see any effort to figure out the interaction between the proposed statutory system and the current voluntary structures that are already in place.

Third, the lack of coordination is important in a second sense, for this statute shows no awareness of how its damage provisions tie in with all the other features of the elaborate network of contracts that bind all parties to the credit system. Thus, there is no awareness that the shift in liability on this score could easily force a shift in the payment of interchange fees that form the backbone of the current system, not to mention all the other specific provisions that bind the relationship together.

In sum, it seems clear that the various forms of legislation will add a new layer of cost and uncertainty to the payment card system. In its present form, the law appears as though it favors banks over retailers, and in the short run that must surely be the case. But in the long run we think that any such legislation is likely to introduce serious distortions, first because of its high administrative costs, and second because of its unintended incentive consequences on the relevant parties. We have no doubt that there is a strong role for government to play in the curbing of theft and fraud, which is the first

⁴⁹ See, e.g., Visa's penalties on non-compliant actors.

leg of any coherent legal approach to cybersecurity. But we are most doubtful that government has much use in the second leg of that policy—the allocation of loss among private players—when that issue has already been the subject of an exhaustive and systematic approach by the parties who are first in the line of fire.