

Information Security Policy in the U.S. Retail Payments Industry

Mark MacCarthy
Georgetown University

Workshop on the Economics of Information Security
June 2010

I. Introduction

The United States retail payments industry is in the middle of a transition in regards to information security. A substantial number of data breaches have occurred over the last five years, despite substantial compliance with the industry standard, the Payment Card Industry Data Security Standard. There will need to be a move to a higher level of security, and the major challenge is institutional. How can the industry organize itself to move collectively toward this goal? Without recommending any particular technical solution, this paper proposes one way to do meet this institutional challenge. Drawing on the experience of Europe and the United Kingdom in moving to a chip and PIN environment, I recommend a public-private partnership where industry, government and civil society jointly work through the technical, economic and public policy issues that need to be solved if we are to have improved information security in the industry.

This paper is organized as follows. In Part II, I look at the information externalities in the retail payment system. This section provides some industry and legal background. It discusses information security as a third party indirect liability regime, and it assesses the system externalities and liability rules that create misaligned incentives for investments in information security. In Part III, I review the Payment Card Industry Data Security Standard, including examples of its data security rules. I discuss levels of compliance and validation, and review some of the data security breaches that have occurred despite the success in moving the industry toward compliance. In Part IV I discuss some public policy issues including mandated cost recovery schemes, data notifications laws, specific security laws, action by the Federal Trade Commission to treat security lapses as unfair acts, and general security laws that require reasonable levels of security. In Part V, I discuss end-to-end encryption and chip and PIN as possible upgrades to the current system, and conclude with a recommendation for a public private partnership to explore ways to move the system forward to higher levels of information security. In Part VI, I conclude with a recommendation for a way forward involving government as an active convener of public-private coordinating groups seeking to guide industry upgrades in information security.

II. Information Security Externalities in Retail Payments

Industry Background

Payment card networks are private, contractual systems that provide a platform linking merchants who accept cards for payment and cardholders who use them to pay for goods and services. Payment systems include unitary enterprises such as American Express and Discover, and independent companies such as Visa and MasterCard that link separate financial institutions into an electronic payment network.¹

Payment systems such as American Express link the two-sides of the payment card market directly. They issue cards to cardholders and they sign up merchants to accept their payment cards. Independent network-forming companies such as Visa and MasterCard are different. They do not have direct relationships with cardholders and merchants. These relationships are maintained directly by financial institutions that are parts of the payment networks created and maintained by these companies. Card issuing banks (“Issuers”) provide network payment cards to cardholders. Acquiring banks (“Acquirers”) sign up merchants to accept network payment cards. They are so named because they “acquire financial transactions for settlement.”

A typical payment card transaction involves an authorization message sent from the merchant where the card is being used to the financial institution that provides processing services for the merchant. The message is routed through the network’s communications and computer systems to the bank that issued the card to the customer. The issuing bank authenticates the card information submitted in the message and authorizes the transaction after ascertaining that the cardholder has sufficient funds or credit. The issuing bank might decline the transaction for a variety of reasons: the identifying information might not be accurate, the Issuer might have blocked the account so as to not authorize transactions (because the card has been reported lost or stolen, or because the account is not current with payments), or the cardholder might not have sufficient funds to cover the transaction. In the case of credit card transactions, sometime after the initial authorization of the transaction, a second process routed through the payment system clears and settles the transaction, transferring funds from the cardholder’s financial institution to the merchant’s account at his payment card bank.

Cardholder information related to these transactions is retained by the financial institutions in the payment system. The merchant’s Acquirer retains information relating to all the purchases made at that merchant, including the cardholder account number of those who bought goods or services from the merchant. The cardholder’s financial institution (Issuer) retains enough information regarding the cardholder’s transactions to send the cardholder a monthly statement. For a variety of reasons including the traditional financial institution duty of safeguarding the accounts of its customers, the severe reputational risk to financial institutions that do not protect customer confidentiality, the tradition of financial industry regulatory oversight, and a variety of specific regulations

¹ Both Visa and MasterCard evolved from an earlier association organizational structure to independent public companies. MasterCard made this transition in 2006; Visa in 2008. A good review of the history and functioning of payment card networks is David Evans and Richard Schmalensee, Paying with Plastic, Second Edition, MIT Press, 2006

(described in the next section), financial institutions have undertaken substantial investments in information security to protect their customer's data, including cardholder data.

However, cardholder information is also retained at the edges of the payment system. The merchants who accept payment cards sometimes retain cardholder information, as do the third-party processors who act as agents both for merchants and for financial institutions in the payment system. These entities are not traditional financial institutions and so do not have the long tradition of customer confidentiality, and are not subject to a general scheme of examination and regulation as are financial institutions. They do not have the same incentives to safeguard cardholder data as do the financial institutions that are part of the payment system. They do not have financial customers; indeed, sometimes, in the case of processors, they do not have retail customers at all because their customers are banks or merchants. So they are less subject to reputational risks than financial institutions and payment card companies if there is a data compromise. Moreover, the allocation of liability within the payment card systems means that they do not pay the full costs of a data compromise, but are able to shift some of these costs to other participants in the systems.

Legal Background: Consumer Protection

Federal consumer protection laws and regulations guide the allocation of liability for unauthorized use of payment cards. The two major laws providing this consumer protection are the Truth in Lending Act and the Electronic Funds Transfer Act.

The Truth in Lending Act protects consumers from liability for charges resulting from the unauthorized use of their credit cards. The Board of Governors of the Federal Reserve System implemented these requirements through Regulation Z.² The Electronic Fund Transfer Act provides, among other things, consumer protections for the use of debit cards. The Board of Governors of the Federal Reserve System implemented these protections through Regulation E, which limits a consumer's liability for an unauthorized debit card transfer from his account.³

In addition to these legal protections, there are also protections that are provided voluntarily by the private payment systems. Zero liability is a good example. For credit

²The Truth in Lending Act (Pub. L. No. 90—321; 15 U.S.C. 1601) was originally passed by Congress in 1968. Major amendments to TILA were made by the Fair Credit Billing Act of 1974, the Consumer Leasing Act of 1976, and the Truth in Lending Simplification and Reform Act of 1980. The implementation through Regulation Z is found at 12 CFR226.12. TILA also requires creditors to investigate and promptly correct billing errors that consumers allege have occurred in connection with their accounts, and entitles consumers to maintain against a creditor much the same claims that they might assert against a merchant in connection with the purchase of defective or otherwise unsatisfactory goods and services.

³The EFTA (Pub. L. No. 96-630; 15 U.S.C. § 1693 *et seq.*) was passed by Congress in 1978. Regulation Z can be found at 12CFR205.11 Regulation E also establishes procedures that a consumer may employ to remedy alleged errors that occur in connection with his account. Regulation E does not provide redress to a consumer who has purchased allegedly defective goods or services using a debit card.

cards, Regulation Z limits cardholder liability for unauthorized transactions to \$50. For debit cards, under Regulation E the liability can be higher depending on when the customer notifies the bank. However, Visa, MasterCard, and the other payment systems have adopted a policy of zero liability in case of unauthorized transactions. This applies to credit cards, debit cards and pre-paid cards. Cardholders are not responsible for transactions that they did not authorize under these private sector policies.

The fundamental reason for these extensions can be summed up in one word: competition. Visa, MasterCard, American Express, and Discover all compete for cardholder loyalty. Consumer protection is an essential element in this competition because it increases consumer confidence in the use of their payment card. This competition for consumer business and loyalty has moved the entire industry to higher levels of consumer protection.

Federal and State Data Security Regulations

Federal and state laws currently apply in this area, but are subject to various limitations and gaps. Generally, financial institutions are subject to data notification and information security rules at the federal level, while non-financial institutions are subject to data breach notification rules at the state level and are subject to a variety of federal information security rules.⁴ The survey of current Federal and state laws indicates that public policy has moved beyond leaving the development and enforcement of information security standards relating to the U.S. retail payment industry entirely to the private sector.

Financial institutions are subject to regulatory requirements with respect to their security practices. The Financial Services Modernization Act of 1999 often referred to as the Gramm-Leach-Bliley Act (“GLBA”)⁵, for example, requires that financial institutions ensure the security, confidentiality and integrity of personal information collected from their customers.⁶ The Federal banking agencies have implemented the requirements of this statute for the traditional financial institutions under their jurisdiction.⁷ These implementing regulations establish a process-based approach to security rather than technical mandates. Companies have to have a written information security program, it has to be overseen by the company’s Board of Directors, and it has to have various components for identifying and assessing risks, and then managing and controlling these risks. There has to be a process for adjusting the program in light of changes in risks and vulnerabilities. To make sure that companies working as agents for financial institutions were covered, the regulations required financial institutions to oversee their service providers, including offshore agents.

⁴ See Congressional Research Service, Information Security and Data Breach Notification Safeguards, July 31, 2007 for a good review.

⁵ Pub. L. No. 106-102, 15 U.S.C. § 6801-6809.

⁶ Id. at § 501(b).

⁷ 66 FR 8152, January 30, 2001 and FR 8616, February 1, 2001.

The FTC promulgated similar security regulations for the nontraditional financial institutions under its jurisdiction.⁸ The FTC's safeguard rule is also process-based. It requires the company to designate employees to coordinate the safeguards, to identify and assess risks to customer information, to design, implement and test safeguards program, to select appropriate service providers, and to evaluate and adjust the program.

In addition, the Federal Trade Commission has broad authority under Section 5 of their enabling statute to take action against unfair and deceptive acts and practices.⁹ In 2005, the FTC began to charge companies with acting unfairly by failing to provide reasonable security.¹⁰ The FTC's assumption of a quasi-regulatory role over the security practices of non-financial institutions is a major step in moving the marketplace toward higher levels of information security.

On March 23, 2005, the Federal Deposit Insurance Corporation, the Federal Reserve Board, the Office of the Comptroller of the Currency and the Office of Thrift Supervision jointly issued interagency guidance concerning risk-based response programs for unauthorized access to customer information and customer notice. This guidance requires a financial institution, when it becomes aware of unauthorized access to sensitive customer information, to "conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused." If the institution determines that misuse of this information "has occurred or is reasonably possible," the institution will be required to notify affected customers as soon as possible.¹¹ However, these rules do not supersede the requirements of state law, such as those established by the California Breach Notification Statute and some of the other notification statutes passed in 2005.¹²

The states have also been active in this area. In July 2003, California enacted S. B. 1386, the "Security Breach Information Act," which requires companies that electronically store unencrypted personal information on a California resident to notify the resident in the event of any unauthorized access to this information.¹³ S. B. 1386 applies whether the security breach occurs within the state or out of state, and whether the business is located in California or not. The notice is required without conducting a risk assessment to determine whether there is a reasonable risk that the information compromised could be used for identity theft, account fraud or other harm to the data subjects involved. The presence of a safe harbor from notification for encryption of the

⁸ 67 FR 36484, May 23, 2002.

⁹ Section 5 of the Federal Trade Commission Act (15 USC § 45) prohibits unfair acts or practices in or affecting commerce.

¹⁰ The FTC has used its unfairness authority to take action against BJ's, DSW and Choice Point. See Press Release, "BJ'S Wholesale Club Settles FTC Charges," Federal Trade Commission, June 16, 2005; Press Release, "DSW Inc. Settles FTC Charges" Federal Trade Commission, December 1, 2005. Despite this FTC Chairman Deborah Majores has indicated her preference for legislation to allow the FTC to extend their safeguard rule to non-financial institutions.

¹¹ 70 FR 15,736 (Mar. 29, 2005); 15 U.S.C. § 6801(b).

¹² Some of the state bills have a provision that deems a company to be in compliance with the state notification if they adhere to Federal notification rules.

¹³ Cal. Civ. Code Section 1798.82.

data somewhat mitigates this concern, and the implementing regulations association with S.B. 1386 attempt to address this issue by making it clear that notification need only be given when information has actually been acquired in the course of a data compromise.¹⁴

Indirect Liability Regimes

Legal scholars have discussed indirect liability regimes in a variety of contexts. An indirect liability regime holds a person responsible for the wrongs committed by another. There are usually several parties involved in an indirect liability regime: the bad actor, the wronged party and a third party. The bad actor is the person directly involved in causing the harm to the wronged party. A third party, neither the bad actor nor the wronged party is assigned the responsibility to prevent the harmful conduct of the bad actor or to compensate the wronged party for the harm. In a copyright infringement case involving an ISP providing access to an illegal download site, for example, the bad actor would be an the infringing site, the wronged party would be the record companies that owned the music copyrights, and the third party would be the ISP.¹⁵

Indirect liability can be imposed through a variety of legal mechanisms.¹⁶ In a tort damages regime, a third party must pay for harms caused by others either on a strict liability or negligence basis. Employer liability for the harms caused by employees is a standard example. Statute or court decisions can impose liability for monetary damages for specific types of harms. Additionally, statutes can require third parties to take certain specific steps to prevent harms to others. A wide variety of legal structures can be

¹⁴ See California Department of Consumer Affairs, Office of Privacy Protection, Recommended Practices on Notification of Security Breach Involving Personal Information – October 10, 2003 at <http://www.privacy.ca.gov>.

¹⁵ Indirect liability is not the same as holding a person responsible for the external negative effects of his own actions, but it has a resemblance. With a negative externality, a person engages in some action, such as cattle-raising or industrial production, and the spill over effects of that action harm some other party who is not directly involved in the activity. Cattle-raising might hurt the neighboring farmers and industrial pollution might harm innocent parties far and near. In this case, the responsible person's actions are directly causing the harm. He is the bad actor. In the indirect liability case, the responsible person is in some fashion involved in the creation or maintenance of the harm and is also in a position to reduce the harm, either by detecting and deterring it or by reducing his own activity that contributes to it. But he is not the bad actor who is directly bringing about the harm. In a case of indirect copyright infringement, for example, the bad actor is the infringer, while the third party would be some intermediary, an ISP or a payment system, whose activity or service allows the bad actor to commit the infringement.

¹⁶ Lichtman thinks his proposal for ISP liability for cyber security issues could be implemented in “negligence or strict liability, whether it is best implemented by statute or via gradual common law development...” Douglas Lichtman, “Holding Internet Service Providers Accountable,” Regulation Winter 2004, p. 59. Mann and Belzley suggest three possible regimes: traditional tort regime, a take down requirement and a hot list. See Ronald J. Mann & Seth R. Belzley, “The Promise of Internet Intermediary Liability,” 47 William and Mary Law Review 239 (2005) pp. 22-24

usefully viewed as indirect liability regimes, including some privacy requirements¹⁷ and some consumer protection requirements imposed on financial service companies.¹⁸

Information security in US retail payments can be conceptualized through the lens of an indirect liability regime. The bad actors are the hackers who gain unauthorized access to cardholder information and use it to commit account fraud or identity theft. The parties who are harmed are other participants in the system, including the breached entity, the cardholders whose information is stolen, and the merchant where the fraud takes place. It is useful to think of an intermediary payment system collectively as a network of financial institutions and service organizations that together provide the electronic and institutional infrastructure linking cardholders and merchants. The payment participants in the networks run by Visa and MasterCard would be examples of intermediary payment systems. The question then arises what responsibilities for information security rest with the payment intermediaries.

An economic framework, broadly construed and supplemented with suitable considerations of equity, can be a useful way to assess the need for indirect liability for intermediaries in specific cases. The elements of the framework are as follows¹⁹:

Market Failure Analysis Are there substantial transaction costs? Can enforcement be achieved without an indirect liability rule? Can private parties work out enforcement arrangements among themselves? Can third parties effectively work with law enforcement without an indirect liability mandate?

Cost-Benefit Analysis Does the burden on the wronged party or on law enforcement to take enforcement steps exceed the burden on the third parties? Are the costs of enforcement efforts reasonable in light of the reduction in harm? Are there longer-term or dynamic considerations to take into account?

Equity Analysis Do third parties exercise such close control over the harm that they should be held responsible for its mitigation or elimination? Are they blameworthy for not taking steps against it? Is the harm particularly egregious?

System Externalities in Retail Payments

Some have argued generally that externalities in information security – consequences that are external to the individual or company – create incentives for

¹⁷ Some privacy requirements can also be thought of as third party liability regimes. Data controllers have a duty to protect the accuracy and integrity of the personal information under their control (for example, by making sure that it is up to date and current and by responding to data subject complaints of inaccuracy) in order to protect data subjects from harm by third parties who obtain this information from data controllers and use it for eligibility decisions (such as employment, credit or insurance).

¹⁸ These are the consumer protection requirements in the financial services industry noted above.

¹⁹ See Mark MacCarthy, "What Payment Intermediaries Are Doing about Online Liability and Why it Matters," Berkeley Technology Law Journal, forthcoming, Spring 2010.

underinvestment in security.²⁰ One person's lax security practices, for example, might allow his computer system to be used for a denial of service attack against another computer.

Retail payment systems exhibit this kind of technical externality. Damage is not contained at one node of the payment network but affects other nodes. Cardholder information might be obtained at one merchant location and used for card fraud at other merchants. In this way, security vulnerabilities in one part of the payment system merchant or processor location potentially affect merchants, cardholders and financial institutions in other parts of the system.

Some security vulnerabilities rest on the way authentication is carried out in the payment system. In the United States, authentication is carried out using static information contained on the payment card's magnetic stripe. Each credit card has a unique authentication code embedded on its magnetic stripe. This code is called the card verification value (CVV). Because it is a static mathematical function of the card account number and the expiration date, it provides a cryptographic check on the contents of the magnetic stripe. The CVV is electronically checked during the authorization process for card-present sales to ensure that a valid card is present. When a credit card is swiped at a point of sale terminal, the account number, expiration date and this code are sent through the payment card network to the issuing bank. The account number functions as routing information, instructing the payment card system to send the information to the appropriate bank and instructing the bank to examine the appropriate account. The CVV acts as an access code. It says to the bank that access to this account is authorized. If this code is missing, or is not the right code, the issuing bank can decline the transaction.

Hackers who obtain the card account number, the expiration date and the authentication code can make a counterfeit card and use it at other merchant locations. The vulnerability is created by the unnecessary storage of cardholder information, the inadequate protection of needed information while in storage, or the failure to protect information in transit. Any merchant, financial institution or processor in a payment system can create risks for other participants in the system by failing to control this vulnerability.

This vulnerability is international. In many other countries, chip and PIN technology is used for authentication at the point of sale terminal. This technology creates a new authentication code for each transaction and so reduces the risk of counterfeit fraud. However, in order for these payment cards to work internationally, they also contain static information that allows them to be used at magnetic stripe terminals. Hackers can skim this information from the magnetic stripe on the card, make a counterfeit card and use it at merchant locations that use only magnetic stripe terminals.

²⁰ See, for example, Computer Science and Telecommunications Board *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*, National Academy Press, Washington, D.C., 2002, available at <http://www.nap.edu/html/cybersecurity>. See also Anderson, R., and Moore, T. "The Economics of Information Security", *Science* (314:5799), October 2006, pp. 610—613.

Fraud at merchant locations in one country can thereby adversely affect financial institutions and merchants in other jurisdictions.

This vulnerability extends to electronic commerce merchants. In an online payment involving one of the traditional payment networks, the online merchant asks for the cardholder number and the expiration date that are printed on the payment card. In addition, they often ask for the security code on the back of the payment card. This security code is a static function of the account number and the expiration date, but it is different from the number on the magnetic stripe. The intent is to provide evidence that the person has the card in his possession.

Security risks to the entire payment system exist at its weakest link. Security is a system-wide issue. It is not the sum of each node's security effort and it is not the result of the strongest effort. The weakest link in the system can be exploited by hackers to gain information that can then be used at other points in the system. No node is safe unless all have reasonable security.

A crucial fact about the US retail payment system is that its network architecture is centralized. It is similar to the hierarchical structure of the telephone network. It is not an end-to-end system.²¹ The network operator has control over the processes and operations of the system in such a way that significant innovation can only occur from the center. The nodes of the system – the merchants, processors, financial institutions, and cardholders – cannot themselves significantly improve or add to the operations of the system. Innovation requires the permission of the network operator, and substantial network investments, to take place. This general fact about the U.S. payment system as a network means that information security innovations must be orchestrated and guided by the system operator.

Perception of system safety is important as well. How safe one firm is depends crucially on how safe other firms are. If all or most firms in an industry employ stringent security measures, data thieves will tend to go elsewhere, since the probability that the next firm in this industry will have a vulnerability when the 10 previous ones did not is low. All security measures can be defeated by some level of effort. The incentive created by the perception that an industry is vulnerable can encourage data thieves to devote higher levels of effort to break through protective measures. This militates against treating security as a competitive differentiator.

Security vulnerabilities in payment systems are externalities in part because of these technical factors, but institutional rules on liability create and maintain the financial misalignment that allows these vulnerabilities to continue. Security is not just a technical

²¹ The key characteristic of an end to end system is that the nodes can provide functionality: “ The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the end points of the communication system. Therefore, providing that questioned function as a feature of the communication system itself is not possible.” J.H. Saltzer, D.P. Reed and D.D. Clark, End-To-End Arguments In System Design, ACM Transactions in Computer Systems 2, 4, November, 1984, p. 278..

problem arising from the payment system design characteristic that security in one node can create problems in other nodes. It depends crucially on how liability for these vulnerabilities is assigned.²²

Industry Liability Rules

When security vulnerabilities allow unauthorized access to cardholder information, the harm that results is usually card fraud. The hackers usually pass the information on to others who use it to buy goods or services presenting the counterfeit card or the cardholder information as a means of payment, and then do not pay the bill.²³ Legal and industry rules determine who is liable for this card fraud.²⁴

An example illustrates how liability rules work in the U.S. payment system. Suppose a merchant or a third-party processor is hacked and enough cardholder information is acquired by a criminal organization to manufacture counterfeit cards. When these cards are used for fraudulent purposes, Federal law and card company policies ensure that the cardholder is protected and does not have to pay for the fraud involved. Similarly, the brick-and-mortar merchants where the counterfeit cards are used have normally satisfied their obligations under card company rules – a card was presented to them, they submitted the cardholder information to the bank that issued the card for authorization, they received approval to proceed with the transaction, they obtained a signed transaction receipt from the customer. They receive payment for the goods or services fraudulently obtained. Under card company policies, it is usually the financial institution that issued the card that bears the liability for the fraud losses and other costs that result from a data compromise. In the meantime, the merchant who was hacked is not fully liable for the fraud losses and other costs created by the loss of cardholder information.

Liability for fraud is different in the online world. E-commerce merchants bear the loss associated with online fraud. The reasons for this include the fact that no card was presented, online transactions are inherently risky, and the merchant does not have a signature. It is extraordinarily difficult to show that the cardholder was responsible for an

²² Liability rules are only one way to affect the incentives for the production of a good or service. These private incentives are the ones that drive economic decisions. See R.C. Cornes and T. Sandler The Theory of Externalities, Public Goods and Club Goods, Cambridge University Press, 1996: “The economically relevant characteristics of a good or service derive from the structure of incentives provided for its production and/or consumption.” p. 9.

²³ For a discussion of how hackers use cardholder information obtained from data breaches for various kinds of fraud see Kimberly Kiefer Peretti, Data Breaches: What The Underground World Of “Carding” Reveals 25 Santa Clara Computer & High Tech. L.J. 375 (2009) (Peretti) available at <http://www.chtlj.org/sites/default/files/media/articles/v025/v025.i2.Peretti.pdf>

²⁴ For a good discussion of the assignment of liability for card fraud in an online and offline context see N. Bohm, I. Brown, B. Gladman, “Electronic Commerce: Who Carries the Risk of Fraud? The Journal of Information, Law and Technology “ (October 2000) available at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/bohm/.

online order when there is no proof that the goods have been delivered and the cardholder repudiates the transaction.²⁵

One good feature of the legal and industry liability rules is that they protect cardholders from bearing the costs of fraud losses associated with unauthorized use. But it is crucial to understand that the information externality is still present, even when liability rules protect the data subject.

Shifting the liability to someone other than the data subject is good from the point of view of protecting the innocent data subject and from the point of view of providing for the long-term growth of the industry. But moving it to another innocent party, in this case the data subject's financial institution does not change the incentives that lead to the security vulnerability to begin with. Whether it is the data subject or the financial institution that bears the liability is irrelevant from the point of view of the merchant. In either case, the cost has been externalized to another party and does not present itself within the merchant's financial account framework and so cannot lead to the appropriate level of investment. To have that effect, liability has to be focused on the institution that created the vulnerability.

These regulatory allocations of fraud losses, and the competitive forces that have ensured that consumers are even more fully protected than required by law, have another effect. They provided a powerful incentive for card companies to minimize unauthorized use of cards. Substantial investments in very sophisticated computer systems – neural networks – that can detect patterns of fraudulent activity and other fraud reduction technologies are justified by the simple economic fact that the card companies bear the loss if fraud takes place. Innovation in fraud control technology usually rests with the financial institutions and payment networks. The scattered uncoordinated merchants and processors are not in a good position to upgrade the payment system. Hence, placing the liability for fraud losses with those best able to innovate to avoid the losses makes good sense.

The costs associated with a data breach include more than fraud losses. Financial institutions incur costs to monitor their systems for incremental fraud, to notify cardholders of the problem, and in some cases to reissue cards. Legal liability rules do not determine who pays for these costs. In the first instance they are incurred by the financial institutions. Industry cost recovery efforts are beginning to shift some of these costs to the breached entity. Court cases have been filed regarding these costs. Some legislation discussed later shifts these costs to the breached entity.

What happens to the card data when it is stolen? The information is rapidly transmitted to website forums that provide a marketplace for the sale of the compromised

²⁵ See Bohm, Brown, Gladman, op. cit. for a good discussion of online fraud liability. Visa and other institutions have guides to limit online fraud. See, for example, Global Visa Card-Not-Present Merchant Guide to Greater Fraud Control 2009 at <http://usa.visa.com/download/merchants/global-visa-card-not-present-merchant-guide-to-greater-fraud-control.pdf>

information. If they have the security codes and PIN numbers the purchasers can make counterfeit cards which can be used to fraudulently purchase goods and services or withdraw cash from ATM machines.²⁶

III. The Payment Card Industry Data Security Standard

The misaligned incentives for security have been known for years, but the vulnerabilities were not easily exploitable by hackers until the development of computer systems at the point of sale and accessibility of these networks to public communications networks such as the Internet. In reaction to this development, the payment card industry has been developing, implementing, and expanding systematic ways to identify and remedy security vulnerabilities in their payment systems. In December 2004, these efforts resulted in an aligned industry standard, called the Payment Card Industry (PCI) Data Security Standard.²⁷ In September 2006, a further step was taken with the formation of PCI Security Standards Council (PCI SSC), an independent council created by American Express, Discover Financial Services, JCB, MasterCard and Visa to manage the standard going forward.²⁸ This created a truly industry-wide security standard, administered by an entity independent of the particular card companies that originally developed the standard. The openness to the stakeholder community via a formalized feedback process created a more robust and practical standard.²⁹

Basic Requirements

The Payment Card Industry Data security standard consists of twelve basic requirements supported by more detailed sub-requirements. These requirements are:

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software

²⁶ See Testimony of Rita Glavin at the Hearing before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, U.S. House of Representatives, March 31, 2009, pp. 2-3 available at <http://hsc.house.gov/hearings/index.asp?ID=185> pp. 2-3. See also Peretti op. cit. supra note 23. There is little evidence that cardholder information from data breaches has been used for new account fraud, where a fraudster presents enough identifying information to a financial institution to open a new account. See ID Analytics, National Data Breach Analysis, January 2006, p. 4, and pp. 30-33.

²⁷ Statement of Steve Ruwe, U.S. House of Representatives, Committee on Financial Services, Subcommittee on Oversight and Investigations, Hearing on Credit Card Data Processing: How Secure Is It?" July 21, 2005, pp. 2-3.

²⁸ Colleen Frye, "PCI council focuses on security standards and requirements," Computer Weekly.com, September 11, 2006.

²⁹ For more detail on the development of PCI set Mark MacCarthy, Payment Card Industry Data Security Standard, in Proskauer on Privacy Practicing Law Institute, 2009 pp. 16-13 to 16-18.

6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security³⁰

The basic requirements are quite general and at that level of generality do not seem to provide much guidance for security professionals seeking to put in place a reasonable security program for cardholder data. But the detailed sub-requirements provide the precision needed to guide the implementation of a security program, and are specific enough to allow an assessor to determine whether a company's information security program is in fact in compliance with the requirements.

Some features of the PCI standard are important to emphasize. First, the rules are not designed to respond to all information security vulnerabilities. They are designed to guard against a theft-of-assets attack. Companies have to have additional controls in place to guard against other classes of attack, including service disruption or capture and control attacks.³¹ The PCI standard is designed to guard against attacks which involve theft or other appropriation and subsequent misuse of cardholder information. Some requirements have to do with maintaining computer system security; others focus on network security; and still others focus on personnel management issues such as who has access to cardholder data. But all are aimed at preventing theft of assets attacks.

Second, the principle of layers of security is evident throughout. Theft of cardholder data can occur through intrusion into the computer system that houses the data, through interception of data in transit within company networks, through the actions of a trusted insider, or through a combination of different avenues of attack. The rules are designed to guard against all channels of attack, and to put in place protections that can block theft of data even if part of a system is compromised. For example, the requirement to have firewalls is backed up with a requirement to protect stored data, so that if the firewalls are breached the cardholder data has been rendered unusable. The requirement to monitor systems and networks also backs up the firewall requirement – if a hacker evades the network firewalls and installs a malicious script the company's computer system, regular monitoring of the system should be exercised to detect the script.

Third, the requirements track the process requirements set up under Gramm-Leach-Bliley. They require companies to identify and assess risks to customer information, to design, implement and test safeguards program, and to evaluate and adjust the program. The application of PCI rules to service providers is also clear. The

³⁰ The PCI version is available on the PCI website <https://www.pcisecuritystandards.org/index.shtml>

³¹ See Congressional Research Service, "Creating a National Framework for Cybersecurity: An Analysis of Issues and Options," February 22, 2005, pp. 6-8 for a discussion of the distinction between the different kinds of security attacks.

GLB rules specifically mention service providers.³² The PCI rule is that member financial institutions, merchants, and service providers should deal only with PCI-compliant service providers. The PCI rules go beyond the process requirements of GLB, however, in specifying particular measures that must be taken to protect cardholder data.

Protecting Stored Data

A good way to illustrate how PCI works in practice is to see how one particular requirement works. Requirement 3 is to protect stored data. A crucial prohibition is against storage of authentication codes that are present on the magnetic stripe of payment cards. To understand why this prohibition is so crucial it is important to understand how these authentication codes function within the Visa system.³³ Each credit card has a unique authentication code embedded on its magnetic stripe. This code is called the card verification value (CVV). Because it is a mathematical function of the card account number and the expiration date, it provides a cryptographic check on the contents of the magnetic stripe³⁴ The CVV is electronically checked during the authorization process for card-present sales to ensure that a valid card is present. When a credit card is swiped at a point of sale terminal, the account number, expiration date and this code are sent through the Visa network to the issuing bank. The account number functions as routing information, instructing the Visa system to send the information to the appropriate bank and instructing the bank to examine the appropriate account. The CVV acts as an access code. It says to the bank that access to this account is authorized. If this code is missing, or is not the right code, the issuing bank does not authorize the transaction.³⁵

There are, of course, other ways for a merchant to ask a bank to authorize a transaction. Internet merchants or merchants who provide goods and services via mail order or telephone order do not send this code through the Visa system for authorization. Some merchants still use manual imprint machines to process transactions. But almost all face to face (brick-and-mortar) merchant use electronic point of sale terminals. For transactions at these terminals to be processed, the code must be included, because only that code indicates to the issuing bank that a valid card has been presented.

These facts about the role of CVV in authorizing transactions have an overwhelmingly important implication for cardholder information security. Without the CVV code, it is not practical to make a counterfeit credit card that works for face-to-face card present transactions. If this code is obtained along with account number and expiration date, a counterfeit card can be made. Without this code, counterfeit cards cannot be effectively utilized for fraudulent transactions.

³² The FTC's safeguard rule, for example, explicitly says that companies must take "reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and... (must)...require...service providers by contract to implement and maintain such safeguards." See 67 FR 36494, May 23, 2002

³³ MasterCard, American Express and Discover use similar authentication codes for their payment cards.

³⁴ CVV is calculated using the Data Encryption Standard (DES) defined by the National Institute of Standards and Technology (NIST).

³⁵ The transaction might not be authorized for an additional reason: the account does not have sufficient funds.

So the risks associated with saving this code are substantial. A large database that stores account numbers and these authentication codes is a very attractive target for criminal gangs interested in obtaining and reselling card information or in making counterfeit cards. There is no business reason to save this information beyond its use in authorizing the transaction. It is not necessary for fraud prevention purposes or to analyze network or computer reliability, since it has no network routing function, and it has no utility for data mining or other analysis of cardholder transactions.

The prohibition in PCI on saving authentication codes emerges naturally from this risk-benefit analysis. The prohibition on saving debit card PIN information and CVV2 arises from similar reasoning.³⁶ If debit card PIN information is stolen, then counterfeit PIN-based debit cards can be produced and used at point of sale terminals or ATM machines. If the CVV2 code is stolen, then thieves can circumvent one of the online fraud detection tools Visa has created to assure merchant that the customer has a real card in his possession.

Validation and Compliance

The security rules set up a list of fundamental requirements, which are reasonably designed to provide for the confidentiality, integrity and security of cardholder data. The basic responsibility of the merchants and service providers who store, process, or transmit cardholder data is to be in compliance with these requirements. In addition, there is a separate duty within the PCI DSS to validate compliance.³⁷

Compliance is not perfect but it is substantial. For example, at the end of 2007, 77% of Visa's largest merchants in the United States had validated their compliance with the PCI DSS and more than 99% of the largest merchants affirmed they do not retain prohibited account data.³⁸ By the end of 2009, 96% of Visa's largest merchants had validated compliance and 94% of the next largest merchants had validated compliance. Their compliance with the rule against storing prohibited data was 100%. Together these merchants account for 63% of the transaction volume in the Visa system. The compliance rate for the more than 5 million smaller merchants who account for the remaining transactions was described as "moderate."³⁹

There has been considerable discussion of the connection between compliance with PCI and the occurrence of a data breach. Recent large-scale breaches have involved

³⁶ The CVV2 is a unique three-digit code printed on the signature strip on the back of all Visa cards. These codes help merchants confirm that cardholders are in possession of the actual card. Online merchants or telephone merchants conducting transactions when the card is not present can verify that their customers have the actual card by requesting the customer to provide the CVV2 number.

³⁷ See Mark MacCarthy, PCI Data Security Standard, op. cit, p. 16-5

³⁸ See Visa Press Release, PCI Compliance Continued to Grow in 2007 Jan. 22, 2008, at www.corporate.visa.com/md/nr/press753.jsp.

³⁹ Visa, U.S. PCI DSS Compliance Status, December 31, 2009 at http://usa.visa.com/download/merchants/cisp_pcidds_compliancestats.pdf

Hannaford and Heartland and are discussed in the next section. Both companies indicated that their breaches occurred even though their compliance with PCI had been validated. Public statements by Visa distinguish between being in compliance and having compliance validated, saying that they do not know of a case in which a breached entity was in compliance at the time of the breach.⁴⁰ Compliance with PCI is no guarantee of perfect safety. But being out of compliance certainly does increase the risk of compromise.

Security Breaches

These vulnerabilities have led to data breaches and the widespread perception that the industry is not doing enough to prevent them. The most salient of these breaches involved substantial losses of card numbers.

In 2004, BJ's Wholesale Club Stores announced that some of its members might have been affected by a possible compromise in its computer system that could have exposed its members' payment card information. A year later it agreed to settle a complaint from the FTC that it has not protected this cardholder information with reasonable security measures.⁴¹ Their security failures included failing to encrypt consumer information when it was transmitted or stored on computers, failing to use readily available security measures to prevent unauthorized wireless connections to its networks, and saving cardholder information in violation of payment card industry rules.

The specificity of the FTC's criticism of BJ's information security practices relates to the use by the FTC of an industry standard, the Payment Card Industry Data Security Standard, as a guide to best practices in the industry.⁴² The claim was that these practices taken together amounted to a failure to take reasonable precautions to keep cardholder information safe and secure. As a result of this failure, issuing banks suffered financial losses from fraud, card reissuance, and monitoring and notification costs. Cardholders suffered inconvenience, worry and time loss dealing with cards that needed to be replaced. Claims against BJ's amounted to \$13 million. The settlement required BJ's to implement a comprehensive information security program and obtain audits by an independent third party security professional every other year for 20 years.

⁴⁰ Prepared Statement of Chairwoman Yvette D. Clarke (D-NY), and Prepared Statement of Joseph Majka on behalf of Visa at the Hearing before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, U.S. House of Representatives, March 31, 2009, available at <http://hsc.house.gov/hearings/index.asp?ID=185> See also Brian Krebs, Hackers Test Limits of Credit Card Security Standards, Washington Post, April 19, 2009

⁴¹ Todd R. Weiss, "Credit card data breach probed at BJ's stores: A 'small fraction' of customer data may have been compromised," Computerworld, March 19, 2004 at http://www.computerworld.com/s/article/91412/Credit_card_data_breach_probed_at_BJ_s_stores. For further details see of the FTC case, its complaint and the settlement agreement see FTC Press Release, BJ's Wholesale Club Settles FTC Charges (June 16, 2005), available at www.ftc.gov/opa/2005/06/bjswholesale.shtm; FTC Press Release, DSW Inc. Settles FTC Charges (Dec. 1, 2005);

⁴² See the PCI standard at https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

In June 2005 MasterCard announced that Card Systems Solutions, Inc., a third-party processor of payment card information, had experienced a breach of its system that potentially exposed more than 40 million cards of all brands to fraud.⁴³ Congress held a hearing on the issue.⁴⁴ Visa suspended CSSI for failure to provide reasonable security.⁴⁵ When CSSI agreed to sell itself to another company, the combined entity was reinstated.⁴⁶ The FTC had charged that CSSI's lax security practices, including the practice of saving the security code on the payment card magnetic stripe, together constituted an unfair practice. In 2006 CSSI signed an agreement with the FTC to abide by a security program with independent audits for the next twenty years.⁴⁷

In January 2007, TJX Cos., parent of the T.J. Maxx and Marshalls retail chains, announced that there had been a computer intrusion that had compromised a substantial amount of payment card information. According to their Annual Report, the intrusion took place over a number of years, starting in 2005 and ending in January 2007, and could have affected as many as 46.2 million cards.⁴⁸ Subsequent court filings in a court case allege that the number of accounts affected was 94 million. The retailer incurred more than \$550 million in expenses, which included fines, restitution for damages, security remediation, and fraud losses. It experienced a 7.5 percent decline in its stock price and a \$1 billion loss in market capitalization.⁴⁹

In March 2008, Hannaford Brothers disclosed a data breach involving credit cards at its supermarket stores.⁵⁰ According to Hannaford's general counsel Emily Dickinson malware loaded onto Hannaford servers allowed attackers to intercept card data stored on the magnetic stripe of payment cards as customer's used them at the check-out counter.⁵¹

In January 2009, Heartland Payment Systems announced what might be the biggest breach ever, with perhaps as many as 100 million payment card records compromised. It appeared that the hacker had been able to install a sniffer program in the processor's computer network and obtain cardholder information, including security codes, in transit.⁵² Costs associated with this breach could reach half a billion dollars.⁵³

⁴³ MasterCard International, News Release, "MasterCard International Identifies Security Breach at Card Systems Solutions, A Third Party Processor of Payment Card Data" June 17, 2005.

⁴⁴ Hearing on Credit Card Data Processing: How Secure Is It? Subcommittee on Oversight and Investigations, Committee on Financial Services U.S. House of Representatives (July 21, 2005), <http://financialservices.house.gov/hearings.asp?formmode=detail&hearing=407&comm=4>

⁴⁵ Statement of Steve Ruwe, at the CSSI hearing op cit pp. 2-3.

⁴⁶ See Eric Dash, Card Center Hit by Thieves Agrees to Sale, N.Y. TIMES, Oct. 17, 2005; see also Pay By Touch Press Release, Pay By Touch Completes Acquisition of Card Systems Solutions (Dec. 9, 2005)

⁴⁷ FTC Press Release, Card Systems Solutions Settles FTC Charges (Feb. 23, 2006).

⁴⁸ See Form 10-K Annual Report: The TJX Companies, Inc., at www.sec.gov/Archives/edgar/data/109198/000095013507001906/b64407tje10vk.htm

⁴⁹ See Craig Tieken, "PCI DSS and Handling Sensitive Cardholder Data—Why You Care," First Data, 2009 p. 8 available at http://www.firstdata.com/downloads/thought-leadership/fd_pci_whitepaper.pdf

⁵⁰ Ross Kerber, "Grocer Hannaford hit by computer breach," Boston Globe, March 18, 2008

⁵¹ Ellen Messmer, "Details emerging on Hannaford data breach: Malware loaded onto Hannaford servers let attackers intercept credit card data," Network World, March 28, 2008 at

<http://www.networkworld.com/news/2008/032808-hannaford.html>

⁵² See Jaikumar Vijayan, "Heartland Earns Back Spot On PCI-Approved List," Computerworld, May 1, 2009.

Law enforcement is able to deal with some of these incidents. For example, the hackers responsible for several of these breaches were arrested in August 2009.⁵⁴ As one industry observer noted, however, the increased effectiveness of law enforcement will not eliminate the problem. Industry changes are needed.⁵⁵

IV. Public Policy and PCI

The fact that data breaches of enormous size continue suggests that the misaligned incentives in the U.S. payment industry have indeed resulted in underinvestment in security. Hackers discovered the vulnerabilities in payment systems. These vulnerabilities were fixable through sufficient expenditures of resources, but they were not fixed quickly. The costs to fix these vulnerabilities fell on one party in the system, namely, the merchants and processors who stored, processed and transmitted key payment information, while the benefits from remedying the flaws would be experienced by others, namely the cardholders and issuing banks who bore the fraud losses under the current system. Fraud reduction technology continued to limit the losses to issuing banks, but the long-term decline in fraud rates stalled.⁵⁶

A program to address the market failure and misaligned incentives within the retail payment system breaks into two parts. First there is the need to define an appropriate set of reasonable security procedures that should be followed by all who transmit, store, or process payment data. Second, there is a need to define the role of public policy, if any, in enforcing these rules. This Part starts from the assumption that PCI is an appropriate set of reasonable standards and explores what government policy should be with respect to enforcing PCI. Under this assumption, the fundamental improvement that is needed in the system is to ensure compliance with PCI. It is a reliable guide to reasonable security, and public policy must simply make sure it is followed by institutions that do not, on their own, have sufficient incentives to practice good security. In the Part V, I explore possible system improvements that would increase information security and the role of public policy in guiding the retail payment system to make these improvements.

⁵³ Eric Dash and Brad Stone, “Credit Card Processor Says Some Data Was Stolen,” New York Times, January 20, 2009 <http://www.nytimes.com/2009/01/21/technology/21breach.html>

⁵⁴ Brad Stone, “3 Indicted in Theft of 130 Million Card Numbers,” New York Times, August 17, 2009.

⁵⁵ As industry analyst Avivah Litan notes, despite the arrest, conviction and sentencing of the hackers in this case “...long-term improvements in payment systems are definitely called for to help prevent future fraud.” See “TJX/Heartland Hacker’s 20-Year Sentence Not a Major Deterrent,” March 28, 2010 http://www.gartner.com/DisplayDocument?id=1331056&ref=g_fromdoc

⁵⁶ Up until several years ago fraud rates were undergoing a long-term secular decline. For instance, between 1992 and 2004, the fraud rate in the Visa system declined from 15.7 basis points to 4.7 basis points. See Joe Majka and Sergio Pinon, “Credit Card Fraud in the U.S.,” The Nilson Report 8-9 (Mar 2005), quoted in Beales and Muris, p. 124. But the rates have stabilized near this low point. According to Ellen Richey, Global Head of Risk for Visa, as of 2009, “fraud rates in our industry remain near all-time lows.” Remarks by Ellen Richey, Chief Enterprise Risk Officer, Visa Inc. at the Visa Security Summit, March 19, 2009, p. 1 at http://corporate.visa.com/_media/ellen-richey-summit-remarks.pdf

Private Sector Cost Recovery

The PCI standard needs to be supplemented with additional enforcement measures to be effective. One such method is to make sure that the costs associated with a breach are the responsibility of the breached entity.

The costs associated with a breach include fraud losses and also monitoring costs, costs of reissuing the cards, notification costs, and the cost of reputational damage and customer dissatisfaction. Visa and MasterCard have both set up private sector cost recovery programs to allow issuing banks under some circumstances to recover some of the costs associated with a breach from the financial institutions that worked with the merchant or other entity that suffered the breach.⁵⁷ The Visa program for example allows issuers to accelerate their claims against breached entities in the case of non-compliance with the PCI data storage rules.

In addition, card networks have negotiated settlements with breached entities that allow U.S. issues to recover some of the costs associated with these breaches in an accelerated fashion. In November 2007, Visa announced an agreement with TJX to offer an alternative recovery program to U.S. issuers that may have been affected by the TJX breach.⁵⁸ Under the agreement, TJX agreed to pay up to \$40.9 million to fund the cost reimbursement program. In December 2009 Heartland agreed to pay American Express \$3.6 million, and in January 2010, Heartland agreed to pay Visa issuers up to \$60 million to cover the costs of the data breach Heartland Payment system⁵⁹

Cost recovery is one method of trying to provide an incentive for greater security. But merchant resistance to cost recovery will mount and there is a likelihood that the private cost recovery arrangement that works well when amounts are small or when responsibility is indisputable will fail to function efficiently when the amounts are very large or where there is lack of clarity about responsibility. Public policy will need to address this situation.

Several different approaches to improving information security through public policy have been put into place or recommended. This section looks at cost recovery legislation, specific security mandates, data breach notification, action by the Federal Trade Commission, and general security requirement for reasonable levels of information security.

⁵⁷ Visa set up an accelerated cost recovery program in 2006 to facilitate the reimbursement of costs associated with a breach to the issuing financial institutions (*See* Visa Press Release, Visa USA Announces Plan to Speed Fraud Recovery for Financial Institutions (July 20, 2006), at <http://corporate.visa.com/md/nr/press631.jsp>) and expanded it on May 27, 2008 <http://corporate.visa.com/media-center/press-releases/press780.jsp>.

⁵⁸ See “Visa and TJX Agree to Provide U.S. Issuers up to \$40.9 Million for Data Breach Claims: U.S. Visa Issuers Eligible to Participate in Speedy, Alternative Recovery Program,” Visa Press Release, November 30, 2007 at <http://corporate.visa.com/md/nr/press748.jsp>

⁵⁹ Grant Gross, “Heartland to Pay up to \$60 Million to Visa Over Breach,” PC World, January 8, 2010 at http://www.pcworld.com/businesscenter/article/186359/heartland_to_pay_up_to_60_million_to_visa_over_breach.html.

Cost Recovery Legislation

Some statutes create liability for costs associated with a breach for companies that are not in compliance with PCI. The Minnesota law states:

“Whenever there is a breach of the security of the system of a person or entity that has violated this section, or that person’s or entity’s service provider, that person or entity shall reimburse the financial institution that issued any access devices affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to cardholders. . . .”⁶⁰

Industry managed cost recovery program are a step in the right direction. But legislated cost recovery programs are less attractive. The basic difficulty is running the cost recovery mechanism through the court system. The cost recovery programs such as Minnesota’s provides a new cause of action for aggrieved parties to bring court cases. But this creates complex factual and legal issues that could simply result in gridlock. The accused parties could reasonably ask for proof that a breach had occurred, that their systems were the ones breached, that is was a failure on their part that allowed the breach, that harm occurred, that the harm was associated with this breach rather than any other, that the harm was avoidable or capable of being mitigated by reasonable steps that the injured party did not take, and so on. As a practical matter, a standard of care would be needed, and this would put the courts in the position of acting as interpreter of “reasonable” industry practices or interpreting the clauses of industry codes like PCI.

Specific Security Legislation

Some statutes do more than require cost recovery. They pro-actively mandate that data controllers take security precautions. Some are very specific. Minnesota’s statute specifies that

“No person or entity conducting business in Minnesota that accepts an access device in connection with a transaction shall retain the card 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.”⁶¹

Governor Arnold Schwarzenegger vetoed AB 779, a similar California bill, saying,

⁶⁰ MINN. STAT. § 325E.64, subdivision 3, available at

<https://www.revisor.mn.gov/bin/getpub.php?type=s&num=325E#stat.325E.64.0>

⁶¹ MINN. STAT. § 325E.64, subdivision 2, available at

<https://www.revisor.mn.gov/bin/getpub.php?type=s&num=325E#stat.325E.64.0> This precaution of not saving authentication codes is based on the PCI DSS industry standard.

“This bill attempts to legislate in an area where the marketplace has already assigned responsibilities and liabilities that provide for the protection of consumers. In addition, the Payment Card Industry has already established minimum data security standards when storing, processing, or transmitting credit or debit cardholder information. This industry has the contractual ability to mandate the use of these standards, and is in a superior position to ensure that these standards keep up with changes in technology and the marketplace. This measure creates the potential for California law to be in conflict with private sector data security standards”⁶²

In September 2008, the Massachusetts Office of Consumer Affairs and Business Regulation issued final data security regulations pursuant to the comprehensive data security law enacted in 2007. These regulations required, among other things, encryption of data as it passes over public networks. Compliance was required by the March 2010.⁶³

The basic flaw with statutes and proposed bills is that they are too specific. As Governor Schwarzenegger noted, they create the potential conflict between industry standards and legal requirements. It also does not allow for or provide any incentive for upgrades.⁶⁴

Data Breach Notification

Recent data breach notification legislation at the state, federal and global levels is one government response to security breaches. As of December 2009, forty-five states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information.⁶⁵ At the end of 2006, six bills had been reported by various Congressional committees, although none had been enacted into law.⁶⁶ In December 2009, the U.S. House of Representatives passed H.R. 2221, which requires data breach notification. Data breach notification has moved abroad as well. Canada, Australia, New Zealand and the United Kingdom have adopted or are considering adopting data breach notification rules. The European Union is considering such legislation as well.

⁶² .” His veto message is available at <http://gov.ca.gov/pdf/press/2007bills/AB%20779%20Veto%20Message.pdf>.

⁶³ Proskauer Client Alerts, “New Massachusetts Data Security Regulations Go Into Effect on March 1, 2010, February, 18, 2010 at <http://www.proskauer.com/publications/client-alerts/new-massachusetts-data-security-regulations-go-into-effect-on-march-1-2010/>

⁶⁴ For a good criticism of the Minnesota law see Thomas P. Brown and Richard A. Epstein, “Cybersecurity In The Payment Card Industry,” 75 University of Chicago Law Review 203 (Brown and Epstein) at http://lawreview.uchicago.edu/issues/archive/v75/75_1/EpsteinArticle.pdf.

⁶⁵ See the list of state security breach notification laws maintained by the National Conference of State Legislatures at <http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx>

⁶⁶ Congressional Research Service, Information Security and Data Breach Notification Safeguards, July 31, 2007, p. 3.

The effectiveness of notification requirements has been debated extensively. But their basic limitation is clear: they rely on an after the fact mechanism to prompt changes in data security practices. They provide the indirect incentive of bad publicity on the back end as a way to encourage good data practices at the front end. One limitation of this approach is that some companies such as CSSI and Heartland do not have direct contact with the public and so are relatively immune from this mechanism. Another is that it is a relatively weak incentive. The real advantage of data breach notification is that it provides information to consumers which they can use to take remedial action to protect themselves against identity theft. By itself it does not provide a sufficient incentive for good security.

FTC Unfairness Action

Another response to the externalities in the information security area has been a series of actions by the FTC under its unfairness jurisdiction. The basic theme is set out in the FTC's complaint against BJs:

Respondent's failure to employ reasonable and appropriate security measures to protect personal information and files caused or is likely to cause substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was an unfair act or practice.⁶⁷

In March 2008 the Federal Trade Commission settled its complaint against TJX. FTC had alleged that its inadequate security was an unfair act or practice. Among the problems the FTC noted were storing and transmitting personal information in clear text, failing to use readily available security measures to prevent unauthorized access to its in-store wireless networks, not requiring the use of strong passwords or different passwords to access different programs, computers, and networks, failing to use readily available security measures such as a firewall to limit Internet access to its computers, not employing sufficient measures to detect and prevent unauthorized access, including failing to update anti-virus software, and not following up on security warnings and intrusion alerts. The settlement required TJX to establish and document a comprehensive information security program and obtain an audit every two years for the next 20 years.⁶⁸

As a practical matter, the FTC looks to industry standards in general and to PCI in particular as a way of determining whether a set of company practices constituted reasonable security. It does not itself make judgments about reasonable security, but defers to forensic evidence and industry standards to determine whether the level of

⁶⁷ Federal Trade Commission, BJS complaint September 20, 2005 p. 3 at <http://www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf>

⁶⁸ See FTC Press Release, Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers' Data (Mar. 27, 2008), available at www.ftc.gov/opa/2008/03/datasec.shtm

protection was adequate. As industry standards evolve, so will the FTC's standard of enforcement.⁶⁹

Generic Security Requirements

The FTC approach of security enforcement might be a more promising model for further legislation. This approach does not rely on specific security mandates, but keys off of private sector standards for information security. To some extent, this is all that is necessary. However, additional legislative direction might be necessary. One way to implement this idea would be legislation similar to the security provisions of the Gramm Leach Bliley Act. This would require companies to establish an information security program that is designed to protect the confidentiality, security, and integrity of personal information. Companies would be deemed to be in compliance if they had implemented an information security program that is in accordance with applicable generally accepted industry standards. Existing standards such as the Payment Card Industry Data Security Standards would fall under that umbrella, but would not be explicitly required. H.R. 2221, the federal bill that passed the House in December 2009, contains a generic security requirement of this sort.⁷⁰

V. Upgrading the System

If the security situation were static, then the above policy approach of treating PCI as a standard of reasonable security to be backed by enforcement actions by a regulatory agency like the FTC would be a sufficient approach. But a key question is how to handle upgrades to the system to ensure that the right level of information security is being provided. This suggests that something more than a static government role is required.

A Framework For Evaluating Upgrades

When should payment participants invest in security upgrades? The system has a whole should be upgraded when the benefits of doing so exceed the costs of doing nothing further, and moreover, have the greatest positive net benefit over other feasible improvements.⁷¹ This concept applies even if no one party receives enough benefit to pay for the improvement on its own.⁷²

⁶⁹ Other similar cases in which the FTC has taken action against companies under its unfairness authority for failure to practice reasonable security include DSW and CSSI. See FTC Press Release, DSW Inc. Settles FTC Charges (Dec. 1, 2005); FTC Press Release, Card Systems Solutions Settles FTC Charges (Feb. 23, 2006).

⁷⁰ Section 2(a)(1) of H.R. 2221 requires the FTC to "establish and implement policies and procedures regarding information security practices for the treatment and protection of personal information..."

⁷¹This is a standard cost-benefit test, adopting the Kaldor-Hicks concept of efficiency that a change should be adopted when the overall benefits exceed the costs. See Mark Furletti, The Laws, Regulations, and Industry Practices That Protect Consumers Who Use Electronic Payment Systems: Policy Considerations, Payment Card Center, October 2005 p. 3 at <http://www.philadelphiafed.org/payment-cards->

While that is the right decision rule from a social perspective, it is not clear that the private incentives of the payment participants are aligned with the social goal. In a purely private setting, it is the private incentives that determine investment decisions, and a variety of failures might prevent private and social costs and benefits to match up.⁷³ Failure to coordinate to manage risk is one possibility.⁷⁴ Another is unequal distribution of the costs and benefits of improved security. As one industry analyst noted:

“In general it is unlikely that the distribution of the costs of security upgrades will match the distribution of its benefits for banks, merchants, consumers, and government, which limits the extent to which individual incentives can control payment fraud. Moreover, if improvements to security standards for one element of the payment network reduce fraud elsewhere, one group of payment participants may “free ride” on the security upgrades of others.”⁷⁵

Other observers have emphasized the difficulties of coordinating when costs and benefits accrue to different actors in the payment system:

“The primary issue is that an individual participant in an electronic payment network has incentive to implement risk controls that reflect private costs and benefits. But the interrelated nature of participants in the payments network implies that some benefit of individual risk control accrues to other network participants. This implies that the social benefits of implementing risk controls will be greater than the private benefits. From society’s point of view, without some form of policy interference in the payments market, insufficient resources may be applied to controlling risk in payments.”⁷⁶

center/publications/discussion-papers/2005/cppolicy-102005.pdf: “... in an ideal environment, payment system participants would adopt any fraud-reduction strategy that saved the entire system more money than it cost, even if the benefits of such a strategy accrued disproportionately to the parties involved.”

⁷² Ibid. p. 4.

⁷³ See Richard Sullivan, “Can Smart Cards Reduce Payments Fraud and Identity Theft?” Federal Reserve Bank of Kansas City, *Economic Review*, Third Quarter 2008 (Sullivan) p. 55 at <http://www.kc.frb.org/Publicat/ECONREV/PDF/3q08Sullivan.pdf>. “The distribution of costs and benefits across payment participants determines the private incentives to improve methods of payment authorization, but the outcome of those efforts is not necessarily best from society’s point of view.”

⁷⁴ See Bank of England. 2000. “The Bank of England’s Oversight of Payment Systems,” *Financial Stability Review* (December), p. 172. At <http://www.bankofengland.co.uk/publications/fsr/2000/fsr09art8.pdf> : “Risks in payment systems need to be identified, measured, monitored and controlled. The public policy interest in reducing risk may be greater than the sum of the individual interests of members. Even if the members are keen to reduce risk in a system, they may be unable to make the necessary changes because of difficulties in co-ordinating action among themselves.”

⁷⁵ Sullivan, op. cit p. 50

⁷⁶ Stuart E. Weiner, Terri Bradford, Fumiko Hayashi, Richard J. Sullivan, Zhu Wang, and Simonetta Rosati, “Nonbanks and Risk in Retail Payments,” Working Paper 07-02, Research Presentation at the Workshop on Economics of Information Security, June 26, 2008, p. 35 at <http://weis2008.econinfosec.org/papers/Sullivan.pdf>

Finally there is the issue of international spillovers. Data breaches have global impact. If a retailer's data base in the United States suffers an intrusion and cardholder information is acquired, this creates risk for the financial institutions and cardholders whose cardholder information has been accessed. Often, those financial institutions and cardholders are in other jurisdictions. The cross-border nature of data breaches exacerbates the information externalities in this industry and creates practical difficulties in assigning liability for cost recovery. Regulators in other countries are faced with harm to cardholders and financial institutions in their jurisdictions and little in the way of effective recourse.⁷⁷ In this context, international coordination might be needed to move the entire transnational payment system to a level of security that is desirable for the system as a whole. This kind of international coordination seems to be referred to in a recent statement from the UK Payments Administration.⁷⁸

Costs of the Current System

Available information about fraud and expenditures for compliance with PCI security requirements suggest that the current situation is not ideal from the point of view of the social cost benefit test outlined in the previous section. Costs associated with the current system fall on cardholders, merchants, and financial institutions. I look at each in turn.

Costs to Cardholders

Because cardholders are protected from liability for the fraud losses associated with data breaches, it is tempting to conclude that they are not exposed to significant data breach costs. However, as the FTC has noted, cardholders whose information has been compromised in a data breach face "inconvenience, worry, and time loss dealing with the affected cards."⁷⁹

FTC studies have attempted to quantify these harms. In 2003, the FTC estimated the cost associated with existing account fraud, which includes counterfeit fraud, the fraud most often associated with data breaches, at \$160 per incident for out-of-pocket expenses and fifteen hours to resolve the problem.⁸⁰ The FTC's follow up survey for

⁷⁷ For example, the Visa TJX agreement on cost recovery did not include non-US issuing financial institutions. The report by the Canadian Privacy Commissioner, op. cit., discusses some of these issues.

⁷⁸ "Counterfeit fraud losses increased by 18 per cent in 2008, but the growth is markedly down on last year's 46 per cent rise. The vast majority of this fraud is due to criminals stealing card details in the UK to make counterfeit magnetic stripe cards for use in countries yet to upgrade to chip and PIN. The industry continues to apply pressure on those countries such as the US where chip and PIN has still to be rolled out." UK Payments Administration, 2008 Fraud Figures Announced by APACS, March 19, 2009 at

http://www.ukpayments.org.uk/media_centre/press_releases/-/page/685/

⁷⁹ Federal Trade Commission, "BJ's Wholesale Club Settles FTC Charges," June 16, 2005

<http://www.ftc.gov/opa/2005/06/bjswholesale.shtm>

⁸⁰ See Howard Beales and Timothy Muris, Choice or Consequences: Protecting Privacy in Commercial Information, 75 U. Chi. L. Rev. 109 2008 p. 124, quoting the 2003 FTC Identity Theft Survey. Out-of-pocket expenses include lost wages, legal fees, and payments of any fraudulent debts, as well as miscellaneous expenses such as postage.

2005 found that 1.4 percent of the population, representing 3.2 million American adults, experienced existing account fraud.⁸¹ Most of them, 80%, reported that they experienced no out-of-pocket expenses, but 7% reported losing up to \$100, 10% experienced losing up to \$1,000, and 3% experienced losses over \$1,000.⁸² About one third of them (38%) were able to resolve the difficulty within one day, but 8% took more than three months to resolve problems.⁸³ A minority (17%) reported problems other than out-of-pocket expenses or time spent to resolve the issue with the credit card company, including being harassed by collections agents, being denied new credit, being unable to use existing credit cards, being unable to obtain loans, having their utilities cut off, being subject to a criminal investigation or civil suit, being arrested, and having difficulties obtaining or accessing bank accounts.⁸⁴

These are tangible costs of breaches for cardholders. In addition, there are the intangible costs. As the 2010 Javelin study of identity theft notes:

The growth in identity fraud victimization rates over the past year is harmful not only because of the dollar losses, but also because of the emotional impact on the victims. Victimization and the accompanying fear it generates lowers faith in the safety of the system and causes secondary effects, which are demonstrated by changes of behavior, such as avoidance of certain merchants, altered usage of payment types and channels, and severed relationships with primary card companies and banks.⁸⁵

While many fears can be magnified out of proportion to their real danger, in the payment card world perception is often reality. A February 2009 report indicated that about two-thirds of all Americans are extremely or very concerned about other people obtaining and using their credit or debit card information.⁸⁶ While intangible, these fears and a pervasive atmosphere of distrust surrounding the use of payment cards represent real costs to consumers.

Merchant Costs

Merchants incur substantial costs associated with the current system. Despite the fact that they do not immediately incur fraud liability, they face other costs associated with a breach and they face costs of compliance with the current PCI data security rules.

Costs of Breaches

⁸¹ Federal Trade Commission: 2006 Identity Theft Survey Report, November 2007 p. 4 at <http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf>

⁸² FTC 2006 Report, p. 37.

⁸³ FTC 2006 Report pp. 25- 26.

⁸⁴ FTC 2006 Report p. 7.

⁸⁵ Javelin Strategy and Research, 2010 Identity Fraud Survey Report, February 2010, p. 22

⁸⁶ Unisys, UNISYS Security Index: United States March 4, 2009, p. 6 at

http://www.unisyssecurityindex.com/resources/reports/Security%20Index%20Wave%204%20US%20Mar%203-09%20_2.pdf

The costs associated with a data breach are substantial for the breached entity. As discussed earlier in the cases of TJX and Heartland, total costs for a company hit with a large data breach can be as high as half a billion dollars. The Ponemon Institute estimates that these costs have risen steadily from a 2005 average incident cost of \$4.5 million to a 2009 cost of \$6.75 million.⁸⁷ This represents an average cost per record breached of \$202. A major element of this expense is the cost of notification of data subjects required by state law. Law suits are common in these circumstances. In addition, share prices are often adversely affected for substantial periods of time, and consumer loyalty declines. The TJX costs described earlier are typical in this area.

Costs of Compliance

Since many of the security vulnerabilities targeted by hackers are present in the computer and communications systems used by retailers and others accepting payment cards, most of the cost of the security efforts in response to data breaches have been made by these companies in an effort to comply with PCI.⁸⁸ The costs of complying with current PCI standards are significant, both for the individual company and for the industry as a whole. According to a 2008 survey by Gartner Inc., the largest merchants reported spending an average of \$2.7 million on PCI compliance up from \$568,000 in the previous year. The second largest group of merchants reported spending \$1.1 million on PCI compliance in 2008, up from \$267,000. These increases represent a five fold jump in compliance costs in just 18 months.⁸⁹

A major focus of the expenditures is to protect static authentication information. Companies often store the security codes associated with payment card numbers without fully realizing it, and must conduct extensive analyses of their systems to discover where these codes are stored and then they must take steps to remove them or mask them.⁹⁰

The overall costs for all merchants are substantial. In mid-2009, the National Retail Federation estimated that their members alone had spent over \$1 billion to comply with PCI.⁹¹ Gartner estimates the total compliance costs as of the beginning of 2009 at \$2 billion.⁹² Others put the cost as ranging between \$2.6 and \$5.5 billion in 2006.⁹³

⁸⁷ See Ponemon Institute, "Global Data Breach Costs Examined For First Time, April 28, 2010, at <http://www.ponemon.org/blog/post/global-data-breach-costs-examined-for-first-time>

⁸⁸ "Avivah Litan, "TJX/Heartland Hacker's 20-Year Sentence Not a Major Deterrent," March 28, 2010 http://www.gartner.com/DisplayDocument?id=1331056&ref=g_fromdoc

⁸⁹ Avivah Litan, PCI Compliance Remains Challenging and Expensive, Gartner, Inc., May 16, 2008, quoted in Craig Tieken, "PCI DSS and Handling Sensitive Cardholder Data—Why You Care," First Data, 2009 p. 6 available at http://www.firstdata.com/downloads/thought-leadership/fd_pci_whitepaper.pdf

⁹⁰ Ibid. p. 6.

⁹¹ Letter to Bob Russo of the PCI Security Standards Council from the National Retail Federation, et. al., June 9, 2009. quoted in Craig Tieken, "PCI DSS and Handling Sensitive Cardholder Data—Why You Care," First Data, 2009 p. 3 available at http://www.firstdata.com/downloads/thought-leadership/fd_pci_whitepaper.pdf

⁹² Eric Dash and Brad Stone, "Credit Card Processor Says Some Data Was Stolen," New York Times, January 20, 2009 <http://www.nytimes.com/2009/01/21/technology/21breach.html>

⁹³ Sullivan, p. 37.

These costs are likely to grow in the future, as the smaller business move to come into compliance with PCI. The costs of compliance with PCI are smaller for smaller businesses. Gartner estimates that they are \$155,000 as opposed to \$1.1 million for the next larger category.⁹⁴ But there are more of them, 2,500 in the third largest merchant category as opposed to 360 in the largest merchant category and 895 in the second largest category.⁹⁵ There are over 5 million merchants in the smallest merchant category. If on average these very small merchants need to spend just \$1,000 for full PCI compliance the additional cost over and above the current industry costs would exceed \$5 billion per year

As a result, extending full compliance with PCI to all merchants will be substantially more expensive than current levels of compliance. It will be necessary, too, if PCI is the sole method for combating hackers. One message for hackers from the high-profile sentencing of the hackers in the TJX and Heartland case is that a move to smaller more distributed exploits might be safer, since smaller events will not draw forth the substantial law enforcement effort needed to locate and capture the hackers.⁹⁶ A theme at the 2009 Visa information security summit was that hackers are turning to smaller companies as the larger ones devote more resources to security, and that compliance for small businesses is complex and expensive.⁹⁷

Costs to Financial Institutions

A major use of card information obtained by hackers in data breaches is to make counterfeit cards, and to use them to commit in-store fraud at retail merchants.⁹⁸ Card issuing banks are initially the ones to bear these costs. The extent of counterfeit fraud has been estimated by the research firm, Aite, at \$1.35 billion in 2008, accounting for 15.7% of the total \$8.6 billion in card fraud faced by U.S. financial institutions. The overall fraud rate, according to the study, was 0.4% of \$2.1 trillion in charge volume in 2008, and had been stable for several years.⁹⁹ But there is some indication that counterfeit fraud has been growing in recent years.¹⁰⁰ It is likely, therefore, that this fraud rate would be substantially lower in the absence of the fraud resulting from data breaches.¹⁰¹

⁹⁴ PCI Cost of Compliance Blog, Cost of PCI Compliance, February 17, 2009 at http://blog.elementps.com/element_payment_solutions/2009/02/pci-compliance-costs.html

⁹⁵ Visa, U.S. PCI DSS Compliance Status, December 31, 2009 at http://usa.visa.com/download/merchants/cisp_pcidds_compliancestats.pdf

⁹⁶ Avivah Litan, "TJX/Heartland Hacker's 20-Year Sentence Not a Major Deterrent," March 28, 2010 http://www.gartner.com/DisplayDocument?id=1331056&ref=g_fromdoc

⁹⁷ Visa, 2009 Global Security Summit: Summary Report, 2009 at http://corporate.visa.com/_media/visa-security-summit-summary.pdf

⁹⁸ See Kimberly Kiefer Peretti, Data Breaches: What The Underground World Of "Carding" Reveals 25 Santa Clara Computer & High Tech. L.J. 375 (2009) pp. 391-392.

⁹⁹ Digital Transactions News, Card Industry Has a Compelling Case for Data Encryption, Report Says, January 13, 2010 <http://www.digitaltransactions.net/newsstory.cfm?newsid=2420>. Card not present fraud accounted for 16.1% of fraud losses and cost \$1.39 billion in 2008. Fraud from lost and stolen cards amounted to an estimated \$1.42 billion, 16.5% of all fraud.

¹⁰⁰ In Canada counterfeit card fraud rose from 37% of credit card fraud in 2006 to 49% in 2008. Compare the Royal Canadian Mounted Police statistics Payment Card Partners Losses by Type 2008 at

In addition, financial institutions bear substantial additional costs, including the costs of monitoring their systems for fraud, the cost of notifying cardholders of breaches, the cost of replacing cards and reputational damage. These costs are often at issue in the law suits that financial institutions bring against breached entities. They are recognized as part of the private sector cost recovery programs run by the payment card networks, and are allowed as possible costs for recovery under state statutes allowing a cause of action for data breach cost recovery. While these costs and the fraud losses might ultimately be shifted to the breached entity through cost recovery programs and legal action, the process is lengthy, procedurally complex and uncertain. The presence of these private law cost recovery programs, legal efforts to recover costs, and further movement for mandated cost recovery under state law all indicate that the financial institutions feel that the current levels of fraud and other costs resulting from data breaches are not acceptable.

The intangible costs to consumers mentioned above also have an important effect on the growth and stability of the payment card industry itself. Payment card companies live on trust as well as convenience. Data breaches, the widespread publicity they receive and the individual notifications that reach the public pursuant to data breach notification laws all contribute to an atmosphere of distrust and fear that can reduce the willingness of consumers to use payment cards.

Summary of Cost Issues

Despite all these costs, the incidence of existing account identity theft appears to be increasing. Javelin reported that the rate increased from 2.5% in 2008 to 2.8% in 2009 and attributed the increase to “increasingly global, hierachal and sophisticated criminal enterprise that specializes in developing new weapons of attack.”¹⁰²

Merchants are increasingly resistant to the need to maintain continuous expenditures to keep their systems in compliance with an ever-changing array of hacker threats. They have attacked the PCI system as overly prescriptive and ineffective.¹⁰³ Their representatives denigrate the PCI standard as simply risk shifting. As David Hogan representing the National Federation of Retailers said at a Congressional hearing:

In our view, if you peel off all the layers around PCI Data Security Standards, you will see it for what it is – in significant part, a tool to shift risk off the banks’ and credit card companies’ balance sheets and place it on others. It is their

<http://www.grc-rcmp.gc.ca/count-contre/cccf-ccp-eng.htm> with earlier RCMP statistics maintained by SpamLaws at <http://www.spamlaws.com/credit-fraud-stats.html>

¹⁰¹ As noted earlier supra at note 56, fraud rates were undergoing a long term secular decline until several years ago when they stabilized near their all-time low point.

¹⁰² Javelin Strategy and Research, 2010 Identity Fraud Survey Report, February 2010, p. 22, p. 8.

¹⁰³ Eric Ogren, “Heartland breach highlights PCI limitations,” SearchSecurity.com, February 5, 2009 at http://searchsecurity.techtarget.com/news/column/0,294698,sid14_gc1346993,00.html

payment card system and retailers -- like consumers -- are just users of their system.¹⁰⁴

The current system has produced dissatisfaction on all sides. Financial institutions look at merchants and see them as failing to take simple and obvious steps to prevent data breaches. They feel they are the victims of merchant carelessness, and seek to remedy this through cost recovery schemes or implicit or explicit mandates for compliance with PCI.

Merchants feel as though the financial institutions are imposing information security requirements on them whose costs are far in excess of the gains generated for these financial institutions. Instead of fixing their payment system security issues, they think, financial institutions are simply trying to shift the cost of providing security to merchants. From their point of view, the PCI compliance issue is entwined with the ongoing contentious dispute between card companies and merchants over the proper level of fees paid by merchants for the use of payment cards.¹⁰⁵

The widespread dissatisfaction with the current system has prompted substantial industry discussions about how to upgrade information security practices of the retail payment industry. Some upgrade and reform is in the works. The question is what. Two ways of improving the current information security system for U.S. retail payments are under active discussion. One is end-to-end encryption. The other is chip and PIN.¹⁰⁶

End-to-End Encryption

A brief background introduces the idea of end-to-end encryption. One of the requirements of PCI DSS is to encrypt transmission of cardholder data across open, public networks. Cardholder data can be intercepted “in flight” as well as obtained from data storage. The same risk of the creation of counterfeit cards exists if the data obtained in transmission include the sensitive authentication codes. However, the transmission of this information as part of the authentication process has a crucial business rationale: Without transmitting the information to obtain an authorization of the transaction, merchants cannot be assured that they are dealing with a legitimate payment card or that the cardholder has sufficient funds to cover the transaction. The solution is to protect the

¹⁰⁴ Testimony Of David Hogan On Behalf Of The National Retail Federation at the PCI hearing at <http://hsc.house.gov/SiteDocuments/20090331141945-95866.pdf>

¹⁰⁵ Congress addressed this “interchange” issue in the Senate version of the financial reform legislation by requiring, among other things, the Federal Reserve Board to examine debit card interchange rates for reasonableness. The controversy will continue as regulators look at the level of interchange to determine if it is reasonable. See Brady Dennis and Ylan Q. Mui, Senate Passes Amendment On Debit And Credit Card Swipe Fees, Washington Post, May 14, 2010 at <http://www.washingtonpost.com/wp-dyn/content/article/2010/05/13/AR2010051303571.html>

¹⁰⁶ An excellent discussion of end-to-end encryption and chip migration is in Smart Card Alliance, End-to-End Encryption and Chip Cards in the U.S. Payments Industry September 2009 at <http://www.smartcardalliance.org/pages/publications-end-to-end-encryption-and-chip-cards-in-the-us-payments-industry>

cardholder data in transmission through encryption. The PCI DSS requirement sets out particular ways to do this.

But this PCI DSS encryption requirement by itself is not sufficient. It covers only transmission over public networks. It does not apply to transmissions within private networks. While cardholder data can be protected by not storing it and by encrypting it when sending it over public networks, cardholder data may still be at risk while it is in transit internally on the entity's network. A network sniffer is a common component in the hacker's toolkit. A hacker can install a sniffer on the entity's network, but needs access to the network to do so.

A series of layered controls responds to this vulnerability. Strong perimeter controls in the PCI standard should impede the hacker's access to the network. The requirements related to perimeter security controls work together with the requirements focused on data protection to provide a layered approach to security. Other requirements in the standard relate to monitoring and testing networks further illustrate this principle of layered security. If a hacker penetrates a network's perimeter controls, effective monitoring and network testing should quickly discover the intrusion and prevent extensive access to cardholder data.

Despite this possibility that complete application of all elements of the PIC DSS would have been sufficient, the hacker in the Heartland data breach was able to successfully obtain substantial cardholder information. End-to-end encryption responds to this vulnerability by encrypting data in transit within private networks. Observers point out however that this is not a replacement for other data security measures and that vulnerabilities exist whenever the data is decrypted.¹⁰⁷

Heartland reacted to the breach in its computer system by endorsing the idea of end-to-end encryption.¹⁰⁸ Visa has endorsed an end-to-end approach as an extra layer of security.¹⁰⁹ It appears to be less expensive than a move to chip and PIN. Aite estimates it would cost \$4 billion to implement over a two year period. It would eliminate about \$2.5 billion in fraud, giving it a payback period of about a year and a half. It would cut some PCI compliance costs but the new-terminal implementation costs would be born by merchants.¹¹⁰

¹⁰⁷ See John B. Frank, Visa Releases Global Data Encryption Best Practices, PIN Debit News, October 5, 2009 at <http://pindebit.blogspot.com/2009/10/visa-releases-global-data-encryption.html>

See also Linda McGlasson, Heartland Data Breach: Is End-to-End Encryption the Answer? Experts Say New Measure is a Start, but Industry Standards are Needed Bank Info Security May 11, 2009 at http://www.bankinfosecurity.com/articles.php?art_id=1455

¹⁰⁸ See its website E3Secure for a description of its program at <http://www.e3secure.com>. For a fuller discussion of this issue see Julia S. Cheney, Heartland Payment Systems: Lessons Learned from a Data Breach, Payment Cards Center, January 2010 at <http://www.philadelphiafed.org/payment-cards-center/publications/discussion-papers/2010/D-2010-January-Heartland-Payment-Systems.pdf>

¹⁰⁹ See Visa, Visa Best Practices, Data Field Encryption, Version 1.0, October 5, 2009 at http://corporate.visa.com/_media/best-practices.pdf

¹¹⁰ Digital Transactions News, Card Industry Has a Compelling Case for Data Encryption, Report Says, January 13, 2010 <http://www.digitaltransactions.net/newsstory.cfm?newsid=2420>

The limitation of the end-to-end approach is that it does not change the fundamental difficulty in the system, which is static authentication. It also leaves substantial responsibility for ensuring safety and security of information with the entity that has possession of it. In the current payment card structure, that means obligations on the merchants and processors. But the current system is not the most efficient. Millions of independent entities who are not expert in information security matters have to make initial and ongoing investments in information security in order to defeat attempts by hackers to obtain information that can be used for fraud. This suggests a better system design is required. In particular, a system that does not rely on static authentication would mean less ongoing monitoring and investment by the fringe actors in the system. The system would be secure by design, not by retrofitting the edges of the system.

The Movement to Chip and PIN

Chip and PIN is one way to implement a dynamic authentication system. In other countries the move to this higher level of security was accomplished through government coordination and approval. Liability shifts and financial incentives for merchants to adopt new point of sale equipment facilitated the transition. A government role to coordinate a similar transition is needed in the United States.

Chip and PIN Overview

Chip and PIN technologies have two parts: a chip part and a PIN part. The PIN part of the system is the requirement of input by the cardholder of a PIN number as part of the authentication process. In the United States this is widely used in ATM cards and in PIN-based point of sale transactions. In addition to a magnetic card reader, the point of sale terminals and ATMS need pads for cardholders to enter their PIN numbers. This is an example of a two-factor authentication system, one that works on the basis of the card, which the person has, and something not on the card, namely, the PIN number which the cardholder knows.

The chip part of the chip and PIN system refers to a variety of technologies that include a microprocessor on the payment card to generate encrypted information and a point of sale terminal capable of generating and receiving this information.¹¹¹ There are many different variations in this technology, but the fundamental idea is that dynamic information is used to authenticate the transaction. In a regular transaction using magnetic stripe technology, the authentication is static. The primary account number, the expiration date, and the cardholder verification value on the magnetic stripe are the same

¹¹¹ To guide the movement to chip and PIN technology and to maintain the same level of acceptance enjoyed by cardholders, payment networks established the EMV (Europay, MasterCard, and Visa) standard. This standard was adopted in 1999. EMV is a standard that ensures interoperability and acceptance of payment system integrated circuit cards (IC cards) of IC-capable POS terminals and ATMs for authenticating credit and debit card payments on a worldwide basis. The EMV standard defines the interaction at the physical, electrical, data, and application levels between IC cards and IC card processing devices for financial transactions. The standard is now managed by EMVCo, which is currently operated by JCB International, MasterCard Worldwide, and Visa, Inc

for each transaction. In a standard implementation of chip and PIN, however, the point-of-sale terminal communicates with the payment card and the card generates an authentication code using a formula that enables the point-of-sale terminal, or host system at the issuing bank, to ascertain whether the code is the expected one. During the next transaction, a different authentication code is generated.¹¹²

The use of chip and PIN has implications for data security. If chip transactions use dynamic authentication codes that change with every new transaction, then thieves who obtain stored cardholder information or information in transit are not able to use that information to engage in a new chip transaction or to manufacture counterfeit chip cards. One result of this is that, in jurisdictions where chip and PIN is prevalent, counterfeit fraud tends to be lower than in jurisdictions where this technology is not used as widely.

In effect, the use of chip transactions is a form of data devaluation. In a country that fully supports chip technology, the compromise of cardholder data is of limited use in the card-present environment due to the dynamic nature of the card authentication.

It does not follow that rules on protecting data storage and encrypting information in transit are irrelevant. Terminals have to be backward-compatible with magnetic stripe cards for the indefinite future; so the stored information from magnetic stripe cards can be used to make counterfeit magnetic stripe cards that are still usable in all terminals worldwide. And some new transactions will generate magnetic stripe data that, if not fully protected, can create a risk of unauthorized use and counterfeit card manufacture.

Both elements, chip and PIN, are needed for a robust defense against card fraud. Chip provides the opportunity for dynamic data authentication, which makes sure that a new authentication code is provided for every transaction. It is designed to prevent counterfeit fraud. Most data compromises are the result of hackers seeking enough information to make a counterfeit card. Dynamic authentication reduces the incentive to break into merchant and process systems to obtain cardholder information. Even if the hacker could obtain information in storage or in transit it would not be enough to make a counterfeit card, since the chip card requires new information for every transaction.

PIN is needed as well. PIN requires the cardholder to enter a static identification number. Lost or stolen cards could still generate accurate dynamic authentication data. Without PIN these lost or stolen cards could still be used for face to face fraud. PIN makes that much more difficult, since without knowing the PIN number the lost or stolen card would be useless for a face-to-face transaction. This second factor - something the cardholder knows – is aimed at reducing lost or stolen card fraud.¹¹³

¹¹² This technology is used in the United States in the contactless payment card implementation by Visa, MasterCard, and American Express to ensure that the authentication code transmitted wirelessly from the contactless card to the point-of-sale reader is different every time. As a result, even if it is intercepted the cardholder information transmitted cannot be used to perform another contactless transaction or to create a counterfeit card.

¹¹³ There is no guarantee that a PIN system is perfect. Researchers at Cambridge University have been able to make chip and PIN transactions without knowing the PIN. See at Richard Evans, "Chip and pin: is your money safe from hackers?" Telegraphy.com.uk, February 19, 2010 at

It might be argued that the key to driving down the value of static authentication information is not the generation of new information each time, but the use of information that is not on the card itself. A second factor – something the cardholder knows – would be enough to render the value of stored information useless. This is the way PIN- based debit cards work. The PIN isn't stored on the card, but is known to the cardholder. There is no chip generating a new authentication code for each transaction.

The problem is that the PIN is still static information. If it can be obtained and associated with the rest of the card details, then counterfeit fraud is still possible. Several ways to do this are known. Even when the cardholder's PIN is transmitted in encrypted form (a PIN block) as part of the transaction authentication process in a point-of-sale transaction, the PIN information can be obtained. Criminals hack into a retailer system, steal the PIN blocks (the encrypted PIN data) and the terminal code that is used to encrypt the PINs. They also steal the magnetic stripe data on the back of the card. With this information, the crooks make up counterfeit cards that can be used at an ATM machine or another retailer.¹¹⁴ Retailers should not save the PIN blocks¹¹⁵ but many do and it creates a vulnerability.

Another way to obtain PIN numbers is through the cardholder's financial institution. Reports from financial institutions involving PIN fraud have recently increased. Fraudsters are targeting the automated telephone banking or voice response unit (VRU) systems of financial institutions to change or obtain PIN information. After obtaining a valid PIN, fraudsters can then make unauthorized withdrawals at ATMs.¹¹⁶

When PINS are compromised, they can be used to access ATM machines as well as point of sale retail terminals. "In recent years, criminal carding organizations engaged in what is known as "PIN cashing" have developed sophisticated "cash-out networks" in which stolen financial information is immediately disseminated to designated groups of criminals who withdraw money from ATMs all over the world within a short time period. In one example, PIN cashers made 9,000 withdrawals worldwide totaling \$5 million in less than 48 hours from four compromised prepaid debit card accounts."¹¹⁷

<http://www.telegraph.co.uk/finance/personalfinance/borrowing/creditcards/7272083/Chip-and-pin-is-your-money-safe-from-hackers.html>. See also Steven J. Murdoch, Saar Drimer, Ross Anderson, Mike Bond, "Chip and PIN is Broken" 2010 IEEE Symposium on Security and Privacy available at <http://www.cl.cam.ac.uk/research/security/banking/nopin/oakland10chipbroken.pdf>. This vulnerability might not have been exploited on a wide scale yet, but it points to the need for financial institutions to be careful in assuming that fraud involving PINs must have involved cardholder negligence.

¹¹⁴ Donna Banks, "Another Money Scam: PIN Block Fraud," Readers Digest.com at <http://www.rd.com/your-america-inspiring-people-and-stories/pin-block-fraud/article26417.html>

¹¹⁵ Visa PIN Security Best Practices for Merchants 2007 at <http://usa.visa.com/download/merchants/pin-security-080507-final.pdf>

¹¹⁶ Visa Inc., Fraud Alert Personal Identification Number (PIN) Attacks, February 5, 2009 at http://usa.visa.com/download/merchants/20090205_pin_attacks.pdf

¹¹⁷ Testimony of Rita Glavin Homeland Security Hearing, p. 3.

Cards need to be issued with both chip and PIN and static magnetic stripe capability. Even after all locations in a given jurisdiction have moved to chip and PIN terminals, cards will still need magnetic stripe functionality. Local cardholders need to be able to use the card at any location that accepts that card brand. Many locations abroad do not have chip and PIN yet. In this way, magnetic stripe functionality is needed to preserve global interoperability.

ATM machines and POS terminals also need magnetic stripe capability. Foreign issued cards often do not have the chip and PIN feature and are usable only at terminals with magnetic stripe capability. To preserve global merchant acceptance magnetic stripe capability is needed at all chip and PIN terminals.

Implementation costs of shifting to the new system are considerable for all parties. For the issuer, authorization and clearing systems have to be revamped and cards have to be re-issued. This is not a one time cost:

Some sources estimate that it costs at least 30 % more to produce and deliver a chip card to a cardholder as compared to a magnetic stripe card. Others put the cost of producing a chip card at somewhere between \$1 and \$3 dollars compared to 13 cents for its magnetic stripe counterpart. Whichever you believe, the incremental cost is considerable.¹¹⁸

For the acquirer, system changes include message protocols and terminal download processes. All POS and ATM terminals in the field have to be either upgraded or replaced. Authorization host systems have to be enhanced, retested and recertified with the card networks. Batch processing systems have to be modified to handle new data elements and to ensure that clearing transactions are properly processed.¹¹⁹ Networks and retailers have costs as well.

The rough dimensions of the cost of the transition are obviously relevant to the question of whether such a substantial investment is worth the cost. It is hard, however, to make precise estimates of the costs of transitioning to a chip and PIN system. Costs to the merchants in England have been estimated at £1 billion.¹²⁰ Others have put the implementation costs in the United States at \$10 billion.¹²¹

¹¹⁸ See O-C Group, EMV: How might the investment be reaped, 2007 at <http://www.ocgroup.com/publications/emv.pdf> p.4

¹¹⁹ Ibid. p. 4

¹²⁰ Sean Poulter, "Chip and PIN was meant to beat credit card fraud. Guess what? It's up 50%" Mailonline.com, March 20, 2009 at <http://www.dailymail.co.uk/news/article-1163167/Chip-PIN-meant-beat-credit-card-fraud-Guess-Its-50.html>.

¹²¹ Speer & Associates, Inc. estimated this cost to be over \$10 billion in its March 29, 2008 issue of *Strategic Commentary*. See Susan Herbst-Murphy, Maintaining a Safe Environment for Payment Cards: Examining Evolving Threats Posed by Fraud, Conference Summary Payment Cards Center, April 2008, footnote 7, p. 15 available at www.philadelphiahfed.org/payment-cards-center/events/conferences/2008/PCCAprEvolvingThreatsFraud.pdf

A recent study of the U.S. market¹²² by Aite estimated that the transition to chip and PIN would cost \$12.7 billion and take three years. Most costs would fall on the acceptance side for installing chip-reading terminals, but issuers also would need to replace mag-stripe with chip cards. The estimated payback would be nearly five years based on an estimated \$2.6 billion in fraud avoided annually could be counted on to cut about 30% of fraud losses by nearly eliminating counterfeit and lost-and-stolen card fraud.

Process of Movement Toward Chip and PIN

The European Commission moved toward greater security in several stages. In 1998, it issued a report inviting the payment system industry as a whole to “enhance the security intrinsic to the payment product on offer, the systems for the processing of transactions originated thereby...”¹²³ In 2001, it issued an action plan, calling for the introduction of chip cards:

“The Fraud Prevention Action Plan has at its heart close cooperation between the relevant public authorities and private parties, exchange of experience and information, training, development and sharing of educational material.

Prevention is primarily a task of the payment systems industry (payment schemes, issuers, acquirers and manufacturers of payment instruments). The most important improvements are technical enhancements e.g. the introduction of chip cards.

However, the Action Plan covers preventive measures that are most effective if implemented in partnership with all parties concerned e.g. holders of payment instruments, retailers and infrastructure network providers, national and international authorities, including law enforcement agencies.”¹²⁴

The motivation was the increasing fraud problem. At the time its fraud rate was .07% of sales.¹²⁵ But in 2000 fraud in the European Union grew by approximately 50%.¹²⁶ The Commission noted with favor the commitment of Visa and Europay/MasterCard to complete the transition to chip and PIN technology in the European Union by 2005.¹²⁷

¹²² Digital Transactions News, Card Industry Has a Compelling Case for Data Encryption, Report Says, January 13, 2010 <http://www.digitaltransactions.net/newsstory.cfm?newsid=2420>

¹²³ Communication from the Commission to the European Parliament, the Council, the European Central Bank and the Economic and Social Committee - A framework for action on combatting fraud and counterfeiting of non- cash means of payment, July 1, 1998, p. 14 at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:1998:0395:FIN:EN:PDF>

¹²⁴ Communication from the Commission to the Council, the European Parliament, the European Central Bank, the Economic and Social Committee and Europol - Preventing fraud and counterfeiting of non-cash means of payment, February 9, 2001, p. 3 at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0011:FIN:EN:PDF>

¹²⁵ Ibid. p. 9

¹²⁶ Ibid. p. 2

¹²⁷ Ibid. p. 5 and 10

In 2004, the Commission issued a further action plan.¹²⁸ It reported a decline in the growth of card fraud from 50% per year in 2000 fraud to 15-20% in 2004, attributable to the increased efforts of the payment industry and national authorities in implementing fraud reduction measures.¹²⁹ The 2004 plan continued its emphasis on chip and PIN: “The migration to chip cards in the EU within a reasonable timeframe would increase security, help reduce fraud and boost user confidence. It is a priority which requires concerted efforts by all stakeholders. The Commission and national authorities should be prepared to assist the migration to chip cards in the EU, if necessary.”¹³⁰

This move to chip and PIN was a combined effort of national authorities and payment systems. The 2004 plan was drafted in consultation with the Fraud Prevention Expert Group of the European Payment Council.¹³¹ FPEG includes EU payment schemes, banks, national Ministries and Central Banks, law enforcement agencies (including Europol and Interpol), the European Central Bank, retailers, consumer groups and network operators.¹³²

The move to chip and PIN was also part of the movement to set up a European payment area. In their first report the EC said: “The SEPA Card Framework (SCF) supports EMV as the technical norm because of the higher security level it offers through the use of chip and PIN.”¹³³ In their second progress report, the EC was even firmer: “The EPC SEPA Cards Framework (SCF) supports EMV as the technical norm because of the higher security level it offers through the use of chip (in combination with a PIN) instead of magnetic stripe. Therefore, SCF compliant cards, POS terminals (point-of sales) and ATMs (automated teller machines) will have to migrate to EMV by end of 2010.”¹³⁴

Liability Shifts and Interchange Incentives

To assist the movement toward chip and PIN, and because of the increased security offered by the EMV technology, the payment networks in Europe introduced a “liability shift.” This provides an incentive to move all terminals and all cards toward compliance with chip and PIN. The liability for fraudulent transactions will pass to the party that is not EMV-compliant in the case of lost, stolen, or counterfeit cards.¹³⁵

¹²⁸ Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee, the European Central Bank and Europol - A new EU Action Plan 2004-2007 to prevent fraud on non-cash means of payment, at

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0679:FIN:EN:PDF>

¹²⁹ Ibid. p. 3

¹³⁰ Ibid. p. 5

¹³¹ Ibid. p. 3

¹³² Ibid. p. 4

¹³³ 2008 SEPA Progress Report, p. 15.

¹³⁴ 2009 SEPA Progress Report, p. 10.

¹³⁵ See European Payments Council, World Report 2006 at

www.europeanpaymentscouncil.eu/documents/World%20Payments%20Report%202006.pdf.

The idea behind the liability shift was to give an incentive to the early adopter on either side of the market. At the beginning of the transition, the liability rests with the issuer and at the end of the transition, when all cards and terminals are chip and PIN, the liability again rests with the issuer.¹³⁶ In the transition, the liability rests with the laggard. If the terminal is not chip and PIN compliant, but the card presented is, then fraud liability rests with the merchant. If the terminal is chip and PIN compliant, but the card presented is not, then liability rests with the issuer.

Europe moved to the new liability regime on January 1, 2005.¹³⁷ So did the United Kingdom.¹³⁸ Visa Canada's liability shift is scheduled for October 2010.¹³⁹ Asian/Pacific countries and countries in Latin America, Central Europe, the Middle East, and Africa all have plans in place to migrate to chip use over the next several years using a liability shift to provide an incentive.¹⁴⁰ The United States is the last major market not moving to chip and PIN.¹⁴¹

The card networks also use an interchange shift to provide an incentive to move to chip and PIN.¹⁴² Merchants who did not install chip and PIN compliant terminals would pay a higher interchange fee when the card used was chip and PIN compliant. For example, if the non-compliant merchant would ordinarily pay 110 basis points for a transaction, they would pay 120 basis points for a transaction when a chip and PIN compliant card was presented. Conversely, merchants would pay a lower interchange fee

¹³⁶ A good discussion fraud liability rules under the current system can be found in Duncan B. Douglass, An Examination of the Fraud Liability Shift in Consumer Card-Based Payment Systems, *Economic Perspectives*, Vol. 33, No. 1, 2009 at http://www.chicagofed.org/digital_assets/publications/economic_perspectives/2009/ep_1qtr2009_part7_douglass.pdf. See also and also Robert G. Ballen and Thomas A. Fox, 2008, "The role of private sector payment rules and a proposed approach for evaluating future changes to payments law," *Chicago Kent Law Review*, Vol. 83, No. 2, pp. 937–952 at http://www.cklawreview.com/wp-content/uploads/vol83no2/Fox_Ballen.pdf

¹³⁷ Robin Arnfield, "Here Comes EMV," *Credit Card Management*, January 1, 2005 at <http://business.highbeam.com/137021/article-1G1-127432153/here-comes-emv-world-watching-new-year-europe-takes>. The Visa chip mandate schedule is part of its International Operating Regulations which can be found at Chip Mandates, March 29, 2007.

¹³⁸ See Chip and PIN "Shift of liability for Fraudulent Transactions," [http://www\(chipandpin.co.uk/business/card_payments/means/shift_liability.html](http://www(chipandpin.co.uk/business/card_payments/means/shift_liability.html)

¹³⁹ J.C. Williams, "The Implications of Chip and PIN Migration," January 2007 p. 11 at http://www.visa.ca/chip/merchants/resources/downloads/chip_study_0207.pdf

¹⁴⁰ The Visa liability shifts for the different regions shifts can be found in their International Operating Regulations Chip Mandates, March 29, 2007. The MasterCard schedule at https://mol.mastercard.net/mol/molbe/public/login/ebusiness/smart_cards/one_smart_card/chip_migration_strategy/liability_shift.jsp

¹⁴¹ "The one major market not yet moving to EMV is the U.S., where low fraud rates make it difficult to justify the cost of converting to smart cards," Denny Jensen, Visa International Senior Vice President of Chip Implementation in Here Comes EMV, op. cit. note 133 supra.

¹⁴² Vidyalaxmi and Preeti R Iyer "Visa, MasterCard want banks to pursue EMV technology" *Business Standard*, January 17, 2006 at <http://www.business-standard.com/india/news/visa-mastercard-want-banks-to-pursue-env-technology/234665/>. MasterCard's interchange shift can be found at https://mol.mastercard.net/mol/molbe/public/login/ebusiness/smart_cards/one_smart_card/chip_migration_strategy/liability_shift.jsp

if a non-compliant card was used with one of their compliant terminals. For example, if the compliant merchant would ordinarily pay 110 basis points for a transaction, he would pay only 100 basis points when a non-compliant card was used. This has the same “laggard” effect as the liability shift, providing a financial advantage to the party that moves first and a financial penalty to the party that delays. At the end of the transition, however, the interchange fee structure returns to its pre-transition levels.

Does the liability shift affect consumers? The chip and Pin program set up by the UK banking industry to manage the transition to chip and PIN answered the question about liability for consumers directly: “There is no change in liability for the cardholder. Consumers remain fully protected from the cost of card fraud, provided they have not been negligent, as they are fully covered by the Banking Code.”¹⁴³

The current version of the banking code, renamed the Lending Code has a section on unauthorized use which seems to preserve the immunity of cardholders from liability.¹⁴⁴ It appears to limit the liability of cardholders for unauthorized use to £50 “unless the subscriber (the financial institution) can show that the customer acted fraudulently or with gross negligence”¹⁴⁵

The problem is that banks are able to hold cardholders liable if they determine that there was gross negligence on the part of the cardholder, and critics have charged that banks have uniformly assumed gross negligence whenever fraud involving a PIN takes place.¹⁴⁶

Compliance and Effectiveness

The compliance rate is substantial and increasing. In 2008, 62% of cards issued in the European Union were compliant, 68% of point-of-sale terminals were compliant and 83% of automated teller machines were compliant.¹⁴⁷ By the end of the second quarter of 2009, those numbers had increased perceptibly. Compliance for cards stood at 72%, 77% for point of sale terminals and 93% for automated teller machines.¹⁴⁸

¹⁴³ Chip and Pin Programme, Consumer Information Frequently Asked Questions at <http://www.chipandpin.co.uk/faqs/affect.html#when1>

¹⁴⁴ Lending Standards Board, The Current Lending Standards, 2009, p. 16. at <http://www.lendingstandardsboard.org.uk/thecode.html>

¹⁴⁵ Lending Standards section 113 p. 16 at <http://www.lendingstandardsboard.org.uk/thecode.html>

¹⁴⁶ Bankrate.com “Are chip and PIN credit cards coming?” in 2010 Credit Card Guide, at <http://www.bankrate.com/finance/credit-cards/are-chip-and-pin-credit-cards-coming-1.aspx>

¹⁴⁷ European Commission, Internal Market and Services DG, Financial Institutions, Retail Issues, Consumer Policy And Payment Systems, Annual Progress Report On The State Of SEPA Migration in 2008, February 2009, p. 15 at

http://ec.europa.eu/internal_market/payments/docs/sepa/progress_report_2008_en.pdf

¹⁴⁸ European Commission. Internal Market and Services DG, Financial Institutions, Retail Issues, Consumer Policy And Payment Systems, Second Annual Progress Report On the State of SEPA Migration in 2009, November 2009, p. 10 at

http://ec.europa.eu/internal_market/payments/docs/sepa/progress_report_2009_en.pdf

The introduction of PIN in UK was very rapid and is now complete. In 2003, a press campaign was launched to manage the transition and tentative deadlines were set.¹⁴⁹ After Valentine's Day 2006 anyone with a chip and PIN card had to know their PIN to be sure they could pay. Banks, retailers and all relevant parties became 100% compliant in 2008.¹⁵⁰

Because UK was one of the most successful in transitioning to the chip and PIN system, it is useful to examine the impact on fraud there. The results seem to show that chip and PIN has been a success. First, fraud at face-to-face merchant locations in the UK is down substantially from £214.8m in 2004 to £98.5m in 2008.¹⁵¹ It continued this decline in 2009 to £72.1m.¹⁵² The need for dynamic information at the point of sale greatly reduced the ability of fraudsters to use the static information on magnetic stripe cards for point of sale counterfeit fraud. This has to count as a great success of the chip technology.

Second, counterfeit fraud itself has been down, then up and then down again. It dropped from £129.7m in 2004 to £96.8m in 2005, but then shot up to £144.3m in 2007 and again up in 2008 to £169.8m. In 2009, it dropped to £80.9m, which is the lowest level since 1999, and a 67% drop since 2004.¹⁵³ The vast majority of the remaining counterfeit fraud is from the use of stolen UK cardholder information at magnetic stripe terminals abroad.¹⁵⁴

Third, the incidence of lost and stolen card fraud is down substantially. In 2008 it reached its lowest level ever recorded.¹⁵⁵ It continued this decline in 2009, and is now

¹⁴⁹ See Chip and PIN Media Alert, January 7, 2003, "The Chip and PIN programme will see magnetic strips on credit and debit cards replaced with a smart chip and by 2005 all UK credit and debit card transactions will be authorised by customers keying in a four-digit PIN rather than signing a receipt." at http://www.chipandpin.co.uk/reflib/new_press_office.pdf

¹⁵⁰ 2009 SEPA Progress Report, p. 20.

¹⁵¹ See UK Payments Administration, 2008 Fraud Figures Announced by APACS, March 19, 2009 at http://www.ukpayments.org.uk/media_centre/press_releases/-/page/685/. The face to face fraud increased in 2008 in part because of account take over fraud, where the fraudster obtains enough information about the cardholder to have replacement cards and new PIN numbers sent to him. It was down 26% in the first half of 2009. See Financial Fraud Action UK, Financial Fraud Action UK announces latest fraud figures, October 7, 2009 at <http://www.banksafeonline.org.uk/documents/2009H1FraudPressRelease.pdf>

¹⁵² U.K. Card Association, New Card and Banking Fraud Figures, March 10, 2010 available at http://www.theukcardsassociation.org.uk/media_centre/press_releases_new/-/page/922/

¹⁵³ U.K. Card Association, New Card and Banking Fraud Figures, March 10, 2010 available at http://www.theukcardsassociation.org.uk/media_centre/press_releases_new/-/page/922/

¹⁵⁴ UK Payments Administration, 2008 Fraud Figures Announced by APACS, March 19, 2009 at http://www.ukpayments.org.uk/media_centre/press_releases/-/page/685/. Counterfeit fraud was down in the first half of 2009, a result attributed to fraudsters increasing their attention to sealing foreign cardholder information and using it at UK locations. Financial Fraud Action UK, Financial Fraud Action UK announces latest fraud figures, October 7, 2009 at <http://www.banksafeonline.org.uk/documents/2009H1FraudPressRelease.pdf>

¹⁵⁵ See UK Payments Administration, 2008 Fraud Figures Announced by APACS, March 19, 2009 at http://www.ukpayments.org.uk/media_centre/press_releases/-/page/685/ : "Lost and stolen card fraud losses decreased by 4 per cent to £54.1 million. Thanks to the introduction of chip and PIN this fraud type is now at its lowest total since the industry collation of fraud losses began in 1991." These losses continued to drop by another 6% in the first half of 2009. See Financial Fraud Action UK, Financial Fraud Action

down 58% from its 2004 level of £89.0m to its 2009 level of £47.9m. The requirement for the cardholder to enter a PIN in conjunction with using a payment card meant that stolen payment cards could not be as easily used for fraud at face-to-face locations. This demonstrates the success of the PIN requirement.

Fourth, online fraud increased from £154.8m in 2004 to £328.4m in 2008.¹⁵⁶ It dropped in 2009 to £266.4m.¹⁵⁷ Apparently, fraudsters were still able to use the static authentication information to commit online fraud and shifted their efforts to this channel of commerce to avoid the extra security precautions that had been introduced in the face to face retail context.

Fifth, fraud on UK issued cards increased at offshore locations from £92.5m in 2004 to £230.1m in 2008.¹⁵⁸ It declined in 2009 to £122.7m.¹⁵⁹ Fraudsters were able to continue to use static authentication information from UK issued cards at off shore merchant locations which continued to use only the magnetic stripe technology.

Finally, UK issuers appear to be able to use chip and PIN to reduce the fraudulent use of their cards at home, but they have been unable to reduce their exposure to card fraud abroad. In 2004, fraud committed using information from cards issued in the UK and taking place at a UK merchant was 82% of the total; by 2008 this UK fraud had dropped to 62% of the total.¹⁶⁰ In 2009, this ratio has increased to 73%.¹⁶¹ It appears that fraudsters were obtaining magnetic stripe information on cards issued in the UK, manufacturing counterfeit cards, but using them abroad with merchants in other countries where chip and PIN were not implemented. UK banks were still liable for these fraud losses, but there was little they could do about it.

Chip and PIN in the United States

UK announces latest fraud figures, October 7, 2009 at

<http://www.banksafeonline.org.uk/documents/2009H1FraudPressRelease.pdf>

¹⁵⁶ UK Payments Administration, 2008 Fraud Figures Announced by APACS, March 19, 2009 at

http://www.ukpayments.org.uk/media_centre/press_releases/-/page/685/. Online fraud decreased 18% in the first half of 2009, a change that authorities attributed to the increased use of Visa and MasterCard online fraud protections. See Financial Fraud Action UK, Financial Fraud Action UK announces latest fraud figures, October 7, 2009 at

<http://www.banksafeonline.org.uk/documents/2009H1FraudPressRelease.pdf>

¹⁵⁷ U.K. Card Association, New Card and Banking Fraud Figures, March 10, 2010 available at

http://www.theukcardsassociation.org.uk/media_centre/press_releases_new/-/page/922/

¹⁵⁸ UK Payments Administration, 2008 Fraud Figures Announced by APACS, March 19, 2009 at

http://www.ukpayments.org.uk/media_centre/press_releases/-/page/685/ Foreign fraud declined in the first half of 2009, a result authorities attributed to the fraud detection systems used by banks and card companies. See Financial Fraud Action UK, Financial Fraud Action UK announces latest fraud figures, October 7, 2009 at <http://www.banksafeonline.org.uk/documents/2009H1FraudPressRelease.pdf>

¹⁵⁹ U.K. Card Association, New Card and Banking Fraud Figures, March 10, 2010 available at

http://www.theukcardsassociation.org.uk/media_centre/press_releases_new/-/page/922/

¹⁶⁰ See UK Payments Administration, 2008 Fraud Figures Announced by APACS, March 19, 2009 at

http://www.ukpayments.org.uk/media_centre/press_releases/-/page/685/

¹⁶¹ U.K. Card Association, New Card and Banking Fraud Figures, March 10, 2010 available at

http://www.theukcardsassociation.org.uk/media_centre/press_releases_new/-/page/922/

The United States payment card industry has not made the decision to move toward chip and PIN in the near future. This does not seem to be a question of not adopting the technology but, as Ellen Richey, head of Visa Risk said in 2009, “a matter of ‘when’ and ‘how.’”¹⁶² Visa seems to be focusing on data devaluation as an achievable goal:

But one thing is clear: the right long-range goal is to make data unusable by criminals – reducing the incentive to steal it. And at Visa, we believe the best way to get there is by introducing dynamic data into the transaction authentication process. Chip is one way to do this. And we’re exploring others.¹⁶³

The United States Congress is becoming interested in the issue. In its hearing in March 2009, the House Homeland Security Committee suggested a move to chip and pin.¹⁶⁴ Chairwoman Yvette D. Clarke (D-NY) noted that the introduction of chip and PIN in UK had reduced fraud in 2007. She then commented:

Despite card fraud dropping 32 percent domestically between 2006 and 2007, overall counterfeit card fraud affecting U.K. consumers was up 46 percent. Why? The cards were being used by malicious actors in countries that had not yet implemented the technology. The U.S. is being blown away by security investments overseas, and our 1950’s era system is making us a weak link in the security chain. Magnetic stripe-based technology is outmoded and inherently less secure when compared to smart cards or other developing technologies. While I am deeply concerned about our security, the payment card industry and issuing banks should be ashamed about the current state of play and doing everything possible to immediately institute improvements in infrastructure.¹⁶⁵

She condemned current industry activities as simply “risk-shifting” and said the time for risk shifting is over.¹⁶⁶

Chairman Bennie Thompson has similar words on investment in chip and PIN and risk shifting:

For the payment card industry and the issuing banks, this is going to mean significant investment in infrastructure upgrades. As the Chair has pointed out, these investments are already occurring overseas. I am puzzled and

¹⁶² Remarks by Ellen Richey, Chief Enterprise Risk Officer, Visa Inc. at the Visa Security Summit, March 19, 2009, p. 5 at http://corporate.visa.com/_media/ellen-richey-summit-remarks.pdf

¹⁶³ Ibid. p. 5

¹⁶⁴ See Hearing before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, U.S. House of Representatives, March 31, 2009, (PCI Hearing) available at <http://hsc.house.gov/hearings/index.asp?ID=185>

¹⁶⁵ See Prepared Statement of Chairman Yvette at the PCI hearing at <http://hsc.house.gov/SiteDocuments/20090331141915-60783.pdf>

¹⁶⁶ Ibid.

disappointed that we are not seeing similar upgrades here domestically, and I hope our witnesses can explain why the card industry appears not to be moving quickly to address these issues. I am deeply troubled by the testimony that suggests credit card companies are less interested in substantially improving their product and procedures than they are with reallocating their fraud costs. The payment card industry's effort to shift risk appears to have contributed to our current state of insecurity, and I am concerned that as long as the card industry is writing the standards, we will never see a more secure system.¹⁶⁷

As the merchant witness at the hearing made clear, from the merchant point of view, the situation is not equitable.¹⁶⁸ Merchants joined the payment system to get guaranteed payment and to increase the volume of their sales. They did not sign on to become information security experts. Now they see themselves forced to invest ever more scarce dollars keeping payment information safe and secure.

From a technical and economic point of view, there is an intrinsic implausibility in a system that distributes enormously valuable information to millions of exposed end points of a network. Especially in a system where the weakest link can cause substantial damage at other links, this network security architecture calls for substantial reworking.¹⁶⁹

If merchants themselves could innovate to resolve this difficulty then putting the burden on them to safeguard static authentication information would make some economic and technical sense. But they cannot. As noted earlier, payment card networks are hierarchical structures similar to the old telephone network. They are not systems that allow distributed innovation in the way fostered by end-to-end systems like the internet. Only network operators in conjunction with end point institutions can facilitate needed innovations.

As noted above, the key answer is that the information has to be made less valuable. Merchants will always have to be security experts to some degree, but the value of static cardholder information is simply too great to expect that they will be able to keep it safe and secure with any reasonable expenditure of resources. The question is how the system as a whole can move to the point where authentication data is unusable for creation of a counterfeit card or for a further transaction.

¹⁶⁷ See Prepared Statement of Chairman Bennie G. Thompson at the PCI hearing at <http://hsc.house.gov/SiteDocuments/20090331141926-86082.pdf>

¹⁶⁸ Testimony Of David Hogan On Behalf Of The National Retail Federation at the PCI hearing at <http://hsc.house.gov/SiteDocuments/20090331141945-95866.pdf>

¹⁶⁹ Industry analyst Aviah Litan makes a similar point "...it's impractical for the card industry to expect the approximately 5 million U.S. retailers that accept credit cards to become security experts and change their systems to fix security holes. Although sensitive retail data should be secured, banks must also own up to the problem and accept responsibility. They must make changes to the payment system so that, even if data is stolen, it is useless to the thieves." See TJX Retailer Data Attack Points to Need for Bank Action, January 23, 2007 available at http://www.gartner.com/DisplayDocument?doc_cd=145963&ref=g_fromdoc

If merchants are reluctant to embrace end user security requirement, there will almost certainly be resistance to the move to a higher level of information security if this involves substantial expenditures of merchant resources. There is some indication that Congressional leaders are sensitive to this concern and would be willing to have the burden placed on the payment intermediary.¹⁷⁰ These cost allocation issues have to be addressed squarely and an equitable arrangement worked out. The ideal set out by Visa's Ellen Richey seems right: this task can only be done in partnership.¹⁷¹ But we seem far from this point. The industry seems caught in disputes over cost allocation rather than in any dispassionate analysis of the costs and benefits of the technology. In this context, there is room for a government role to ensure that all sides have a hearing on the issue and that a movement to an improved level of security is made in a way that reasonably accommodates the interests of all parties.

VI. The Way Forward

The chip and Pin story and the public policy situation in the United States suggest an institutional improvement to guide upgrades. In the United States, the question of upgrades is largely left to the private sector. At one level this is right. Expertise in information security is largely housed in private institutions and consulting firms, not in government agencies. But information security is not simply a technical matter. It is a matter of when improvements in the system can be made at reasonable cost, and how the burdens and benefits of an improvement should be shared. Coordination difficulties, misaligned financial incentives and unequal distribution of the benefits and burdens of system upgrades can all conspire to prevent an upgrade that would be to the betterment of the system as a whole. This is precisely where a positive role for government is required.¹⁷²

Government should not simply be a passive overseer of information security standards developed autonomously by the private sector. It should be an active convener of public-private coordinating groups seeking to explore not only the different technical improvements that could be made to increase information security, but also to examine

¹⁷⁰ See Prepared Statement of Chairman Yvette at PCI hearing op cit. "...the payment card industry and issuing banks need to commit to investing in infrastructure upgrades here in the United States."

¹⁷¹ Richey speech op. cit. p.1: "In this ongoing security battle, partnership is the winning strategy."

¹⁷² Brown and Epstein appear to conclude that no government involvement can do better than the private contracts negotiated by the parties themselves. See Brown and Epstein op. cit. supra at note 63 available at http://lawreview.uchicago.edu/issues/archive/v75/75_1/EpsteinArticle.pdf. However, the only example of failed regulation cited is the extreme Minnesota law which does suffer from the rigidities that a specific mandate has and the inefficiencies that might arise from simply making merchants consequentially liable for damages associated with data breaches. A generalized reasonable security standard enforced by a regulatory agency such as the FTC does not suffer from such limitations. Neither would an attempt to move beyond current technology through a government coordination program. As noted in Paul M. Schwartz and Edward J. Janger, Notification of Data Security Breaches, 105 Mich L Rev 913, 932–45 (2007) at http://www.paulschwartz.net/pdf/datasec_schwartz-janger.pdf government can help by creating and maintaining a coordinated response architecture. Their CRA, however, is limited to supervising and coordinating a notification and mitigation effort. The real concern, however, is for developing new higher levels of security.

the institutional friction that could prevent systematic improvements, and to work with private sector partners to find ways around these friction points.

As discussed earlier, the right way to think about improvements in information security in the U.S. retail payments industry is through the lens of a social cost benefit analysis. The system should move to a higher level of information security technology when the benefits outweigh the costs, regardless of the party on whom the costs and benefits fall. Issues of equity can arise when those who benefit from the transition are not the same as those who must bear the costs. These equity issues can create coordination difficulties that might block the move to a more efficient information security system. They can and should be addressed through a publicly acknowledged and fair cost allocation scheme that allows those who benefit from the transition to compensate those who must bear the costs.

One way to do this is through public regulatory proceedings such as the one that led FFIEC to move toward two factor authentication.¹⁷³ The advantage of this is that it utilizes long established procedures designed to allow and safeguard public input. The disadvantage is that the regulatory model might not be the best in a circumstance where partnership, discussion and dialogue are the right approach. The regulatory approach is also limited in that many parties who would have to participate in efforts to upgrade technology might fall between regulatory cracks.

A second approach would be to build on the formal and informal industry groups that are involved in security in the financial services industry. FS-ISAC¹⁷⁴ and the Financial Industry Sector Coordinating Council¹⁷⁵ are two such entities. These groups meet regularly to exchange best practices and information regarding security threats and have an extensive network of contacts with government agencies already developed. They provide a good example of public private partnerships to address these issues. Their membership, however, is limited to financial service companies or trade associations, and would need to be expanded significantly to provide the right mix of parties.

The industry associations that are involved in information security provide a useful model as well. PCI SCC is heavily involved in the development of information security standards and has access to substantial expertise to evaluate new technologies.¹⁷⁶

¹⁷³ Federal Financial Institutions Examination Council, “Authentication in an Internet Banking Environment,” at <http://www.ffiec.gov>

¹⁷⁴ The Financial Service Information Sharing and Analysis Center is an “industry forum for collaboration on critical security threats facing the financial services sector.” See <http://www.fsisac.com/>

¹⁷⁵ FISCC is a “group of more than 30 private-sector firms and financial trade associations that works to help reinforce the financial services sector’s resilience against terrorist attacks and other threats to the nation’s financial infrastructure.” See <https://www.fsscc.org/fsscc/>

¹⁷⁶ PCI SCC collaborates with a variety of stakeholders in determining when to upgrade PCI DSS. See PCI Security Standards Council Enters Next Phase Of Data Security Standards Development, November 16, 2009 at https://www.pcisecuritystandards.org/pdfs/pr091116_lifecycle_phase_3_and_post_cm_release.pdf

BITS is also an organization that could aggregate and organize industry expertise.¹⁷⁷ The missing piece for these organizations is explicit involvement from government.

Finally, representatives of civil society should be at the table for any industry government discussions in this area are. Academic and public interest groups working in the area should be involved in the technological evaluation, economic assessment and cost allocation discussions because any decisions in this area will affect consumers and the general public. Input from groups that directly represent consumers and the general public is needed.

With this type of industry collaboration with government policy makers and representatives of civil society, the way forward to a higher level of information security will be easier and will be more likely to produce a result that is more efficient and more equitable for all.

¹⁷⁷BITS is associated with the Financial Services Roundtable. It is an industry consortium made up of 100 of the largest financial institutions in the US. It “provides intellectual capital and fosters collaboration to address emerging issues where financial services, technology, and commerce intersect.” See <http://www.bitsinfo.org/>