Testimony of
Mark MacCarthy
Georgetown University
Before the
Health IT Policy Committee
Governance Workgroup
September 28, 2010

My name is Mark MacCarthy. I am adjunct professor in the Communication, Culture and Technology Program at Georgetown University where I teach, consult and conduct research in technology policy, including information security and privacy. Prior to this, I was Senior Vice President for Public Policy at Visa Inc.

Thank you for the opportunity to testify today on the important issue of national health information network governance. In my testimony, I will describe some features of the U.S. retail payments industry that might be of use to your deliberations on constructing a governance mechanism for a national health information exchange. I focus on the Payment Card Industry Data Security Standard (PCI DSS) and standardization efforts within the payment industry.

Let me summarize my major points as follows:

- A centralized security standard setting organization can help prevent industry fragmentation.

- Distinguish the elements of the security program: standard, compliance and enforcement, and assign responsibilities to parties carefully

- A backup government enforcement role might be necessary to supplement industry efforts.

- Pay attention to liability rules. They can provide incentives for security compliance, they can promote innovation, they can protect customers, and they can promote industry growth. They can also bog an industry down in unproductive litigation.

- If standardization is needed in a fragmented industry, a government coordinating role might be necessary

I discuss these points in further detail below, staring with some industry and legal background.

## 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.

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.

## Legal Background

Federal consumer protection laws and regulations guide the allocation of liability for unauthorized use of payment cards. The Truth in Lending Act protects consumers from liability for charges resulting from the unauthorized use of their credit cards. These rules limit liability to $50, although the industry practice is zero liability. The Electronic Fund Transfer Act provides consumer protections for the use of debit cards, and limits the amount of liability to $500, although the liability could be unlimited depending on the time a cardholder notifies its bank of unauthorized use. The industry practice is to treat debit cards and pre-paid cards similar to credit cards and to provide zero liability protection for unauthorized use.

## Need for an Industry Security Standard

The need for an industry security standard emerged from two separate features of payment systems, one technical, the other institutional. Payment systems suffer from substantial security externalities that require a system-wide approach. In addition, the liability rules in the payment networks create misaligned financial incentives that block the needed level of investment in security.

### Security Externalities

Retail payment systems exhibit security externalities. 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 (CCV). 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 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. 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.

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 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.

**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. Legal and industry rules determine who is liable for this card fraud.

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

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.

## Payment Card Industry Data Security Standard

The PCI DSS is a response to the need for an industry-wide security program. The PCI DSS is rightly regarded as a successful self-regulatory program that moved the payment card industry to a higher level of information security. Compliance is not perfect but it is substantial. For instance, 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 priority 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."

The elements of this program are (1) a centralized standard setting organization, called the PCI Security Standards Council, (2) a detailed information security standard, called the PCI Data Security Standard, (3) a program for validating compliance with the standard, (4) an enforcement program, and (5) a liability regime to respond to costs associated with data breaches. I discuss each in turn.

## Security Standards Council

PCI DSS developed out of earlier standards developed by Visa and MasterCard. in the late 1990. Visa's program was called the Cardholder Information Security Program (CISP). Its structure was straightforward: standards, validation of compliance, and enforcement. The program required the financial institutions in the Visa system to ensure that their merchants and agents in all payment channels (brick-and mortar, mail order/telephone order, and e-commerce) complied with these new security requirements. After a period of over a year of development and review, the standard and its associated compliance and enforcement program was released to the industry in September 2000. The effective date was delayed for a period of time to give merchants and processors the chance to upgrade their systems to come into compliance. The program was approved by the Visa Board of Directors and formally introduced into the Visa Operating Rules in June 2001.

There was at this point no coordination with MasterCard or the other card companies. MasterCard proceeded independently, and in 2001 they introduced their own

voluntary cardholder information security program, called the Site Data Protection Program (SDP). It was made mandatory in 2003. MasterCard's SDP was structured in similar fashion to the Visa CISP program—security standards, definitions of categories of merchants and service providers with different validation requirements associated with the different categories, lists of approved security assessors, and a separate enforcement scheme. The MasterCard program, however, focused exclusively on e-commerce merchants, and other merchant channels were not included in its scope. There was a large overlap between MasterCard's SDP program and Visa's CISP program; but the programs were not developed together, and at the beginning they were not coordinated.

As Visa's experience with CISP grew, it became apparent that the lack of coordination with other card companies was slowing the broad adoption of the fundamental security practices needed in the emerging environment. Visa's program had slightly different security requirements, slightly different testing methodologies, and a different vendor certification program. Some merchants felt that they would have to have one security assessment done for Visa and, even though they passed it, would then have to have an entirely new assessment done, using slightly different protocols, by a different vendor for MasterCard. Visa and MasterCard were able to handle these inefficiencies on a case-by-case basis, but by 2004 it became clear that it was time to align the programs.

In December 2004, MasterCard and Visa announced an agreement to align their data security requirements for merchants and third-party processors. This alignment led to the formation of a standard for cardholder information data protection known as the Payment Card Industry Data Security Standard (PCI DSS). American Express and Discover adopted PCI DSS as well. This move to PCI DSS helped merchants and service providers to assess the status of their security by using a single set of security requirements. They were also able to select one vendor and implement a single process to validate their compliance with payment card data security programs. The advantages for them were lower costs and reduced complexity. It was one more step toward promoting wider acceptance of standard security requirements for the industry.

The final step in the evolution of the industry's efforts to promote cardholder security was the formation of a separate standards organization. In September 2006, American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International announced the formation of an independent council designed to manage the ongoing evolution of the PCI DSS. In forming this PCI Security Standards Council (PCI SSC) the five founding members were taking one more step to enhance the payment industry's efforts to secure payment account data in a globally consistent manner. The Council's charter called for it to:

- develop and maintain a global, industry-wide technical data security standard for the protection of accountholder account information
- reduce costs and lead times for Data Security Standard implementation and compliance by establishing common technical standards and audit procedures for use by all payment brands

- provide a list of globally available, qualified security solution providers via its website to help the industry achieve compliance
- lead training, education, and a streamlined process for certifying Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs), providing a single source of approval recognized by all five founding members
- provide a transparent forum in which all stakeholders can provide input into the ongoing development, enhancement, and dissemination of data security standards.

The organization of the PCI Security Standards Council was intended to be transparent and open to all interested industry participants and stakeholders. It is led by a policy-setting Executive Committee, composed of representatives from the founding payment brands. Operational decisions are made by a Management Committee, also from the payment brands. An Advisory Board, drawn from Participating Organizations, provides input to the organization and feedback on the evolution of the PCI DSS.

## Data Security Standard

When Visa was developing its CISP program it needed to develop a specific standard for keeping cardholder data safe and secure. There were very general recommended practices available. One such example was ISO 17799, a set of recommended information security practices, but compliance with these general recommendations could not be certified.

Visa needed to move beyond these general recommendations to a standard that was designed for the preserving the security of payment card information and to assure consumer confidence in the Visa brand and payment system. Such a standard would provide a framework addressing the specific needs of the companies that stored, processed, and transmitted payment card information, and that would be precise enough to allow independent auditors to assess compliance. Visa retained outside security firms to help them develop draft standards, and circulated the proposals to the information security specialists in the major financial institutions that were members of the Visa system. This CISP standard was the one adopted by the Visa Board in 2001.

The early CISP standard evolved into the existing PCI Data Security Standard. 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
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 security

## 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 all parties 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.

Visa requires its client financial institutions to ensure that their merchants and agents perform this validation. Merchants and processors that store, process, or transmit cardholder data must demonstrate that they are in compliance with the PCI DSS rules. One way to do this is to submit an assessment done by a qualified security assessor, and for some merchants and processors such an assessment is required. But the submission of an assessment indicating compliance is not a substitute for actually being in compliance with the security requirements. The validation requirement is in place to provide some assurance to member financial institutions that the rules are being followed. In addition, when an assessment indicates a problem, this can often be a guide to taking steps to come into compliance with the security requirements.

The PCI DSS validation program consists of three components: onsite inspections, self-assessments, and network scans. The validation requirements differ according to the level of the merchant or service provider, reflecting the risk-based nature of the validation requirement. The level of a merchant or processor is based mostly on transaction volume. Level 1 merchants, for example, are those with over 6 million transactions per year. It is important to stress that a company must be in compliance with the requirements of the standard regardless of its transaction volume. However, it is more important that a large volume user of the system demonstrate that it is in compliance with the security rules because the harm to the other stakeholders in the system is much greater.

Level 1 merchants must perform annual on-site data security assessments and quarterly network scans. The on-site security assessment can be conducted by an outside security assessor or by an internal merchant auditor. It must compare the security procedures and practices in place in the environment in which the merchant stores, processes, and transmits cardholder data with the requirements of the PCI DSS. There is a document—the PCI Security Audit Procedures—that provides the detailed steps that must be used to complete a Report on Compliance. This report must be provided to the

merchant's financial institution each year to demonstrate compliance and must be available to Visa upon request.

PCI SSC maintains a list of qualified assessors to perform these assessments. To become a qualified security assessor, a company must apply as a firm for qualification in the program; provide documentation of financial stability, technical capability, and industry experience; qualify individual employees to perform the assessments; and execute an agreement with PCI SSC governing performance.

Alternatively, acquirers may elect to accept the Report on Compliance from a merchant's internal auditor, provided that a letter signed by an executive-level officer of the merchant accompanies the report. Smaller, level 2 and 3 merchants must complete an annual self-assessment questionnaire. This questionnaire is keyed to the specific requirements of the PCI DSS.

A network security scan checks systems for vulnerabilities. This scan remotely reviews networks and Web applications based in the externally facing Internet address provided by the merchant. Level 1, 2, and 3 merchants are responsible for ensuring that a quarterly network scan is performed on their Internet-facing perimeter systems by a qualified independent scan vendor. All scans must be conducted by an approved third-party network security scanning vendor and must be conducted in accordance with a defined set of procedures.

Service providers have a tiered set of validation requirements as well. All service providers, regardless of the number of cardholder accounts processed, transmitted, or stored, have to undergo quarterly network scans. Level 1 and 2 service providers must have an annual on-site security assessment done by an independent qualified security assessor. Unlike merchants, they may not substitute an internal audit for the independent assessment. Rather, validation of compliance must be determined by an approved security assessor. Level 3 service providers must complete the annual self-assessment questionnaire. And unlike merchants, they submit their documentation directly to Visa, not to particular financial institutions.

Visa financial institutions must use, and are responsible for ensuring that their merchants use, service providers that are PCI DSS–compliant. Service providers must be registered with Visa prior to inclusion on the list of PCI DSS–compliant service providers. When a company successfully completes a security review based on the PCI DSS, it can be put on the list and is eligible for use by merchants and financial institutions. Reviews are valid for a single year and must be renewed annually; if companies are more than ninety days late in providing their annual report, they are removed from the list.

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 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. Compliance with PCI is no guarantee of perfect safety. But being out of compliance certainly does increase the risk of compromise.

## Enforcement

Enforcement is the third part of the industry information security program. Unlike the standards themselves and the validation process, the enforcement of the standards and the penalties for noncompliance are not part of the PCI DSS. Visa has its own enforcement process and procedures and makes its own judgments about the severity of sanctions that might be appropriate in particular cases. MasterCard, American Express, and Discover all have similar discretion.

A crucial feature of the enforcement regime in the Visa system is the imposition of penalties on the financial institution that is part of the Visa system. Visa does not have contractual relations with merchants or with third-party processors. These relationships are all maintained by the Visa client financial institutions. For this reason, enforcement of all Visa rules is pushed to the edge of the Visa system, to those entities with the direct on-going relationship with the merchants and processors. Decentralization is an efficient way to handle this task. With over 6 million merchants in the Visa U.S.A. system alone, it is better to have the financial institutions in the Visa system enforce the Visa rules on a day-to-day basis. MasterCard has a similar structure and a similar enforcement regime.

The Visa client financial institution has the responsibility for making sure that a merchant or processor is in compliance with the PCI DSS rules and the responsibility to obtain a report of compliance.

Consequently, if a merchant or processor fails to be in compliance with the PCI DSS rules, the penalties for this noncompliance fall on the Visa client financial institution. Depending on the contractual relationship that the member has with the merchant or processor, these penalties can be passed on to the merchant or processor that violated the Visa rules.

There are severe penalties for noncompliance with PCI DSS. If a client financial institution, merchant, or service provider does not comply with the security requirements or fails to rectify a security issue, Visa may fine the responsible financial institution or impose restrictions on the merchant or its agent. Client financial institutions are subject to substantial fines for any merchant or service provider that is compromised and not PCI DSS–compliant at the time of the incident. The rule here is quite clear: It is not enough that a merchant or service provider have provided a report on compliance that indicates that they were in compliance with PCI DSS at some time in the past; the entity must be found to be in compliance with the security rules at the time the incident occurred. In

cases where the noncompliance with CISP rules is egregious, Visa reserves the right to withdraw that entity's ability to process Visa transactions.

## CSSI

A good way to understand the enforcement process is to see it at work in an extreme case, the Card Systems Solutions, Inc. ("CSSI") breach.43 On June 17, 2005, MasterCard announced that CSSI, a third-party data processor, had experienced a cardholder information compromise in which over 40 million card accounts had been put at risk. In Congressional testimony, MasterCard said it had identified a small cluster of fraud that ultimately led it to a certain merchant bank, Merrick Bank. The pattern was ultimately traced to CSSI, a third-party processor used by Merrick Bank. Upon notification, CSSI was able to identify the presence of a malicious computer script in its system. The script was designed to export cardholder data without authorization. Subsequently, an independent data security firm at CSSI conducted forensic analysis. It was determined that CSSI was storing transaction information on its systems in violation of PCI DSS rules, the presence of the malicious computer script was confirmed, other serious security vulnerabilities were detected, and specific evidence was found of a security breach of CSSI's computer network.

Based on the preliminary results of this forensic audit, MasterCard issued a press release to notify the public on June 17, 2005. At around the same time, Visa and MasterCard notified the affected banks of the breach and provided them with lists of the accounts that were potentially at risk. MasterCard required CSSI to bring its systems into compliance with its security requirements by August 31, 2005. Visa took different action. Visa determined that approximately 22 million Visa card accounts from the CSSI database were put at risk. It noted that, in many of those cases, CSSI, by its own admission, had knowingly and improperly retained magnetic stripe information that could be used to help create counterfeit cards, in clear violation of the PCI DSS security rules. As a result of CSSI's egregious failure to follow these security requirements, Visa terminated CSSI's ability to act as a processor for Visa financial institutions. American Express also stopped allowing CSSI to process their transactions.

The incident with CSSI was ultimately resolved through an acquisition. On December 9, 2005, Pay By Touch, a provider of biometric authentication and payment solutions, announced the acquisition of substantially all the assets of CSSI. The combined entity was in compliance with Visa's security rules and is able to process Visa transactions.

## Liability

One method of providing an incentive for compliance with PCI DSS is a liability program that imposes the costs associated with a breach on 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. 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. 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 system

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.

Some state 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. . . ."

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.

## Standardization

Cooperation among payment system competitors on the development of common industry standards spurred the growth of the industry. In 1968, the major payment systems were the fledgling Visa and MasterCard systems and American Express. They worked together with the American National Standards Institute to devise common standards that covered everything from the size of the payment card to the way in which account numbers were encoded on the card's magnetic. ANSI issued the standards in 1973. These industry standards were later given international approval through the International Organization for Standardization. ISO/IEC 7813, for example, sets standards for the account numbering system used on payment cards, while ISO/IEC 7810 dictates physical size. Visa used these industry standards in 1973 when it introduced its BASE I system that allowed merchants to send requests for authorization over telephone lines. American Express and MasterCard system also followed the same standards.

One advantage for the payment industry was that common standards eased the transition for merchants who had to install electronic terminals to process the new magnetic stripe payment cards. If each merchant had to install a separate, incompatible terminal for each payment brand it would have cost them much more. Terminal manufacturers could have incorporated different standards into their terminal equipment, but this would have dramatically increased costs, again slowing the process of adoption. The industry participants saw that it was in their own best interest to adopt common standards as a way to increase the overall size of the market, and then to compete for market share within this larger market. No government requirement dictated this agreement. It emerged naturally from the incentives present in the payment card marketplace.

The incentive for merchants to move to this new, more efficient electronic system was provided through centralized discounts in their merchant fee. Electronification of the process proceeded rapidly starting from the introduction of incentive rates in 1979, reaching 80% by 1990. It is virtually universal today. Open, non-proprietary industry standards available to all participants also facilitated competitive entry. In 1985 when Discover entered the market with a competitive product, they were able to develop a standardized product that worked with existing terminals.

The industry has continued this pattern of developing common standards to facilitate the development of new products. To guide this movement to chip and PIN technology, Europay, MasterCard, and Visa developed the EMV standard in 1999. This standard ensures interoperability and acceptance of chip cards at compliant chip terminals at the point of sale and at ATMs. When Visa, MasterCard and American Express introduced contactless cards in the United States starting in 2005, they all

independently adopted an ISO 14443 standard to govern communications between the contactless card and the new terminals.

This pattern of common standards is highly typical of network industries, and reflects the fact that they are often concentrated markets. While the Visa and MasterCard systems coordinate the efforts of thousands of independent financial institutions, at the network level there have always been a small number of centralized players in the payment system market. Agreement on standards and a willingness to compete within them was easier in such concentrated markets. Coordination difficulties can often prevent less concentrated markets from adopting industry-wide standards. If there is a public interest in industry standards in such contexts, it might be necessary to look for government to play a coordinating role.

## Lessons Learned

Payment system security standards and enforcement mechanisms have been successful and deserve study as models for other industry efforts. Standardization in the payment industry is also instructive. Some lessons that might apply to other industries are the following:

- A centralized standard setting organization can help to prevent industry fragmentation.
- Distinguish the elements of the program: standard, compliance and enforcement, and assign responsibilities to parties carefully
- A backup government enforcement role might be necessary to supplement industry efforts
- Pay attention to liability rules. They can provide incentives for security compliance, they can promote innovation, they can protect customers, and they can promote industry growth. They can also bog an industry down in unproductive litigation.
- If standardization is needed in a fragmented industry, a government coordinating role might be necessary