I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Government and Private Sector Roles in Providing Information Security in the U.S. Financial Services Industry

MARK MACCARTHY*

Abstract. The financial services sector provides an interesting case study for the proper relationship between government and the private sector in the area of information security. Financial information is attractive to thieves; the sector is pervasively and pro-actively examined and regulated; existing federal security rules impose specific process duties on financial institutions; financial regulatory agencies have exercised this authority in various ways from issuing examination guidance that have pushed the industry toward more robust online banking security procedures to using the industry's payment card industry data security standard as a measure of reasonable levels of security. This paper suggests that the legitimate roles of government range from allowing the industry to autonomously develop its own set of security practices to actively encouraging the adoption of specific security measures. However, the government should generally refrain from enshrining specific security measures in law or regulation since it can freeze innovation, lock in less effective security measures, and prevent the development of compensating controls that are less costly and equally effective. A key role should be to assist the industry to move to higher and socially beneficial levels of security in order to overcome various coordination problems that prevent natural industry forces from moving in that direction.

---

* Adjunct Professor, Communication, Culture and Technology Program, Georgetown University, and Vice President for Public Policy, Software and Information Industry Association (SIIA). The views expressed in this article are those of the author and not necessarily those of Georgetown University, SIIA or any of its member companies.

I. INTRODUCTION

In December 2010, the Financial Services Sector Coordinating Council (FSSCC) signed a memorandum of understanding with the Department of Commerce and the Department of Homeland Security.[1] The purpose of this memorandum was to improve security in the financial services industry and, in particular, to set the stage for research and development projects that would facilitate innovation, identify and overcome cybersecurity vulnerabilities, and develop more effective and efficient cybersecurity processes.[2] The memorandum commits the parties to work together cooperatively in projects of cooperation and coordination, information sharing and the development and implementation of joint test infrastructures.[3] The three parties also pledge to cooperate with the U.S. Treasury Department, which leads responsibility for cybersecurity in the financial services sector.[4]

Why is this interesting? It helps illuminate the question of the proper roles and responsibilities of government and industry in the provision of reasonable information security in the financial services industry. The memorandum of understanding provides an outline of the best way to proceed. The key words are cooperation and coordination, where each party recognizes its own area of expertise and works together with others toward a common goal.

This might seem banal and too obvious to be worth discussing, but in fact this model stands in sharp contrast to some typical thinking about the proper role of government and industry in the provision of important goods like information security. On the one hand, some think that government should not be a partner with industry, but should instead play a unilaterally dominating role, determining through regulatory processes the direction and amount of investment

---

[1] Memorandum of Understanding between the Dep't of Homeland Sec. Sci. and Tech. Directory, Dep't of Commerce Nat'l Inst. of Standards and Tech., and Fin. Servs. Sector Coordinating Council for Critical Infrastructure Protection and Homeland Sec. (Dec. 6, 2010), *available at* https://www.fsscc.org/fsscc/reports/2010/FSSCC_DHS_NIST_MOU_12062010.pdf [hereinafter *Memorandum of Understanding*].

[2] *Id.* at 1.

[3] *Id.* at 2.

[4] *Id.*

in information security in the industry.[5] On the other hand, others view the matter as totally within the discretion of industry players. They argue that market forces will set the right level of effort to promote information security in the industry and that the government has no role in coordinating this effort.[6]

This paper adopts the point of view that cooperation and coordination should be the default mode of interaction between key government agencies and the financial services industry. I illustrate this theme through the examination of case studies. The first involves the payment card industry data security standard (PCI DSS). I briefly trace the development of this standard as the product of autonomous industry initiatives. Then, I discuss the use of this standard by the Federal Trade Commission in enforcing its requirement for reasonable information security practices and by state legislatures and regulators as a template for mandatory state information security rules. The second case study involves the guidance issued by federal financial services regulators in the area of online banking. The regulators concluded that single factor authentication, such as static passwords, were insufficient by themselves to defend against phishing attacks, and recommended stronger authentication procedures, including two-factor authentication. The third case study involves the public-private partnership that fostered the development of smart card technology in the European Union. I then draw lessons learned from these case studies, which include:

- Government can have an extraordinarily powerful effect through the establishment of liability rules and regulatory responsibility;

- Regulation and legislation should be at the level of principles with implementation left flexibly to the interaction of industry and government agencies;

---

[5] Part II, *infra*, discusses the Minnesota law on payment industry data security which prescribes as a matter of law very specific security requirements for industry to follow.

[6] *See* Thomas P. Brown & Richard A. Epstein, *Cybersecurity in the Payment Card Industry*, 75 U. CHI. L. REV. 203, 221–23 (2008) (arguing that contracts within the industry will be able to allocate efficiently information security responsibilities without the need for any government coordinating role).

- Government involvement is counterproductive when it locks specific security practices into law or regulation;
- Government has a key role as a convener:
    - It should identify and eliminate coordination difficulties that prevent industry action.
    - These institutional roadblocks will be less about the efficient level of security investments and more about the allocation of costs and benefits associated with moving to a higher level of security; and
- The legitimate government role ranges from low to high involvement:
    - Industry autonomously evolves security standards.
    - An enforcement role putting the weight of government behind industry-developed and upgraded standards.
    - More active phase where government agencies conclude that current industry practices are inadequate and must be improved but does not mandate or promote any particular solution.
    - A more active phase where government actively encourages industry to adopt a particular security approach.

Part II deals with the case studies involving the U.S. payment card industry security standard, the regulatory response to online banking security vulnerabilities, and the European public-private partnership regarding smart card security. Part III draws together the lessons learned. Part IV provides a conclusion.

II. PART TWO

A. PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

All business institutions have a responsibility to keep the information they have on data subjects secure from unauthorized access.[7] In the financial services industry, special features add to this general obligation. First, there is a long history of confidentiality in the industry. Customers of financial institutions have a settled expectation that their information will be held in a confidential fashion and, for generations, bankers and other providers of financial institutions have met these expectations. It is built into their traditions and institutional practices. Second, there are explicit requirements that financial institutions face under current law.[8] These requirements are enforced in the financial services industry through regular examinations of bank practices and processes.

Retail payment systems operated by financial institutions and their service companies live under these obligations as well. These payment systems include the unitary systems operated by American Express and Discover, and the network-forming companies Visa and MasterCard that coordinate the retail payment activities of thousands of financial institutions.[9] In these systems, network operators bring together merchants and customers in a two-sided market. Unitary systems do this directly by providing the ability to accept payment instruments to merchants and the ability to use payment instruments to retail customers. Distributed payments systems do this through intermediary financial institutions that handle the direct relationships with merchants and retail customers.

In both cases, the flow of information through the system is crucial for understanding security threats and vulnerabilities. In a typical transaction, a cardholder swipes a card at a merchant location.

---

[7] The fair information practices adopted by HHS, OECD, FTC, DHS all include reasonable security as a requirement. For an account of the development of fair information practices see Fred Cate, *Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY 342 (Jane K. Winn ed., 2006); *see also* Robert Gellman, *Fair Information Practices: A Basic History*, BOBGELLMAN.COM (Oct. 3, 2011), http://bobgellman.com/rg-docs/rg-FIPShistory.pdf.

[8] *See* Gramm-Leach-Bliley Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified in scattered sections of 15 U.S.C.).

[9] *See* DAVID EVANS & RICHARD SCHMALENSEE, PAYING WITH PLASTIC: THE DIGITAL REVOLUTION IN BUYING AND BORROWING (2d ed. 2006).

Information needed to authenticate the transaction is read off the magnetic stripe of the card by the terminal at the point of sale. This information is transmitted through communications networks and computer systems operated by the payment company. In distributed systems, the information is first routed to the merchant's bank, then via the payment card network to the cardholder's bank. The card number functions as routing information directing the authentication information to the right financial institutions. At the financial institution, the security code embedded in the magnetic stripe functions as an access code. If the code is incorrect or missing, the financial institution can decline the transaction. If the code is correct, and the cardholder's account can support the transaction, the financial institution sends a return message authorizing the transaction. The account number and the security codes are the crucial pieces of information that must be protected by information security systems at each stage of the process--from merchant location to the cardholder's financial institution.

The demand for information security cascades through the layers of the retail payment industry. Distributed payment systems, such as Visa and MasterCard compete with each other for the loyalty and business of financial institutions, and the integrity and security of financial transactions is an essential element of this competition. In turn, financial institutions and unitary payments such as American Express compete for merchant and individual customer business and must provide assurances of merchant security and cardholder information in order to acquire and retain customers in this intensely competitive market.

A third legal element unique to the payment industry reinforces these general pressures toward providing information security. The liability for security breaches that lead to fraud losses typically falls on the financial institutions themselves.[10] Financial institutions that issue payment cards cannot pass the losses associated with unauthorized use of these cards on to the cardholders. They have a clear economic incentive to reduce the security vulnerabilities that can lead to fraud losses. Within the retail payment industry, therefore, existing traditions, industry practices, explicit legal requirements, and liability allocation all move the industry toward higher levels of information security.

---

[10] The Truth in Lending Act protects consumers from liability for charges resulting from the unauthorized use of their credit cards. *See* Truth in Lending Act, 15 U.S.C. §§ 1601-1666 (2010). The Electronic Fund Transfer Act provides, among other things, consumer protections for the use of debit cards. *See* 15 U.S.C. § 1693 *et seq.* (2010).

However, this is not the case with other participants in retail payment service networks. In particular, the payment processors and merchants who are essential links and end points in these networks are not subject to these pressures to the same degree as the financial institutions. For them, a classic economic externality problem lessens their incentive to make cost-effective information security investments. [11] A payment processor, for example, retains large amounts of cardholder information as part of its network responsibilities to transmit, store, and process transaction information. But if hackers gain unauthorized access to cardholder information stored in, or in transit through, the payment processor's systems, payment processors bear no financial liability for any resulting fraudulent activity. This liability is externalized to other parties in the system; primarily the financial institutions who issued the affected cards. A disclosure requirement cannot remedy this externality since these processors typically have no retail customers who might withdraw their business because of information security failures.[12]

The payment card industry data security standard came into existence to remedy this externality. [13] Starting with separate initiatives by Visa and MasterCard in the early 2000s, the standards were eventually harmonized in 2004 and handed over to a separate payment card industry council in 2006. This council, the Payment Card Industry Security Standards Council, now directs the developments and upgrades for the standard, regularly issuing bulletins about the latest security threats, authorizing security assessors, and publishing new versions of the standard.[14]

---

[11] For the classic statement connecting information security issues to economic externalities, see Ross Anderson & Tyler Moore, *The Economics of Information Security*, 314 SCI. 610, 610–13 (2006).

[12] In a typical case, the customers of these processors are merchants or banks that provide payment service to banks who themselves have no liability in the case of data breaches resulting in fraud.

[13] For more detail on this development see Mark MacCarthy, *Information Security Policy in the U.S. Retail Payments Industry*, 2011 STAN. TECH. L. REV. 3 (2011).

[14] *About Us*, PCI SECURITY STANDARDS COUNCIL, https://www.pcisecuritystandards.org/organization_info/index.php (last visited Feb. 27, 2012). The latest version of the standard, issued in October 2010, is PCI DSS version 2.0. *See* PCI SEC. STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARDS (2010), *available at* https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf.

The standard consists of the following three elements: (1) a list of required activities and security measures organized around twelve general security rules; (2) a mandate of validation of compliance with the standard; (3) and enforcement actions taken for failure to comply. The requirements consist of detailed measures to be taken by all entities that store, process or transmit cardholder data. The standard contains rules designed to meet threats and vulnerabilities typically encountered in the payment card environment and specific enough for an independent security assessor to validate compliance. For example, the general rule to protect stored data is made more specific for the payment card environment by the detailed requirement not to store payment card security codes. The storage of these security codes serves no legitimate business purpose and creates the possibility that compromised information could be used to make counterfeit cards.

Compliance with PCI DSS is achieved through private contract. The payment card networks, for example, have a network of contracts with financial institutions that provide services to merchants. These contracts require the financial institutions to ensure that the merchants they service are in compliance with the standard. The validation requirement is also enforced through contract. Each financial institution is required to ensure that its merchant customers provide a report on compliance to them each year. Merchants of a certain size must have a security assessment done by an independent outside vendor. Penalties for failure to comply can include fines and, in extreme cases, a ban on processing transactions.

Success of the program is a matter of dispute. Compliance rates have increased since the start of the program, with large merchants approaching 90% domestically and over three quarters globally.[15] But

---

[15] Maria Bruno-Britz, *PCI Council and Visa See More PCI Compliance*, BANK SYS. & TECH., Dec. 21, 2008, http://www.banktech.com/payments-cards/204802100 (noting that "compliance definitely is trending upward, certainly among large and midsize merchants. Figures recently released from Visa (San Francisco) show that 65 percent of the largest merchants have validated their compliance to the PCI DSS, up from 36 percent in December 2006. Midsize merchants are complying, too, with 43 percent now in compliance compared with just 15 percent at the end of 2006."); Ellen Richey, Statement at the Visa Security Summit (March 19, 2009) (transcript available at the VISA NEWSROOM, http://corporate.visa.com/_media/ellen-richey-summit-remarks.pdf) (By 2009, compliance among large merchant compliance had grown to 90% with almost 100% compliance with the prohibition on storage of security codes.); *see also* Press Release, Visa, Visa Program Encourages Merchant Adoption of EMV Chip as Path Toward Dynamic Authentication (Feb. 9, 2011), *available at* http://corporate.visa.com/media-center/press-releases/press1098.jsp (International compliance is high as well. According to Visa, "More than 76 percent of the world's largest retailers have validated compliance with the security standard."). Even the level of compliance, though, is not free of controversy. Some studies report that two-thirds of the companies that should be in full compliance with PCI are not.

the effectiveness of the program in stopping data breaches is controversial. Visa maintains that ". . . no compromised entity has yet been found to be in compliance with PCI DSS at the time of a breach."[16] The perception that the standard is ineffective stems from the fact that some companies that suffered a breach had validated compliance with PCI. However, forensic analysis of the compromised systems showed that they were not in compliance at the time of the breach.[17] This difference between validating compliance and being in compliance does not indicate an underlying weakness in the standard itself. It might reflect difficulties in the assessment process, which often rely on sample testing of systems and can fail to detect vulnerabilities.

The point of this development for present purposes is that the standard was formulated and diffused through the industry without a government mandate. No government entity dictated the content of the standard or mandated any element of it as the standard was being developed. The industry's reaction to the vulnerabilities at the edges of the payment networks was self-contained and autonomous. This might seem to vindicate those who think that the government should simply stay out of the business of promoting information security in the industry. But that would be a misleading interpretation of the events because it ignores the crucial role played by the Federal Trade Commission in promoting compliance with the industry standard.

A. FEDERAL TRADE COMMISSION ENFORCEMENT

Since 2001, the Federal Trade Commission has brought over twenty-nine cases alleging that businesses had failed to protect consumer information.[18] More significantly, since 2005, they have

---

See Matthew J. Schwartz, *67% of Companies Fail Credit Card Security Compliance,* INFO. WEEK, (April 20, 2011, 1:06 PM), http://informationweek.com/news/security/management/229401946?queryText=credit+card+compliance.

[16] Richey, *supra* note 15, at 3.

[17] Thorough forensic examination of the state of a system at the time of a breach can reveal vulnerabilities that might have been missed in an annual assessment. An assessment is a snapshot, meaning that a system that is actually compliant at the time of an assessment might fall out of compliance later. "[I]t was the lack of ongoing vigilance in maintaining compliance that left the company vulnerable to attack. Based on our findings following the compromise, Visa has taken the necessary step of removing Heartland from its online list of PCI DSS compliant service providers." Richey, *supra* note 15, at 1.

[18] *See Prepared Statement of the FTC on Consumer Privacy: Hearing on Consumer Online Privacy Before the S. Comm. on Commerce, Sci., and Transp.*, 111th Cong. 10-11

brought successful cases alleging that failure to maintain reasonable security is an unfair practice under the section 5 of the FTC Act.[19] In the BJ's Wholesale case, for example, they alleged:

> 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.[20]

From our perspective, the important point behind these unfairness cases is that the industry standard was effectively being used as a standard of "reasonable and appropriate security measures." The specific allegations in the FTC's complaints map onto the requirements of the PCI standard in ways that make it clear that the FTC was relying on the industry standard. For example, in the BJ's Wholesale case, the company was alleged to have "created unnecessary risks to the information by storing it for up to thirty days when it no longer had a business need to keep the information, and in violation of bank rules."[21] This alleged violation is the same as the prohibition on storing cardholder security codes contained in the PCI standard.[22]

As a result of these cases, the legal community began to advise its clients that failure to comply with the industry standard could result in a finding of unfairness by the Federal Trade Commission. It is hard to avoid the conclusion that the improvement in compliance with the PCI standard that took place between 2006 and 2010 was due in part to the strong enforcement efforts of the FTC during the same period.

(2010) (prepared statement of Jon Leibowitz, Chairman, Fed. Trade Comm'n), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_senate_hearings&docid=f:67686.pdf.

[19] *Id.*

[20] In re BJ's Wholesale Club, Inc., No. 042-3160, at 3 (F.T.C. Sept. 20, 2005), *available at* http://www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf.

[21] *Id.* at 2.

[22] *See* PCI SEC. STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARDS, *supra* note 14, at 30.

Without this government enforcement role, it is unlikely that compliance would have been as widespread or as swift.

This use of the FTC's enforcement power as a regulatory backup to a standard developed autonomously by the industry is a good example of the coordination and cooperation needed to move the industry to a higher level of security practice. The FTC staff does not have expertise in information security measures, but it can rely on the standard developed by the industry in determining whether a company behaved reasonably with respect to its security practices. This division of labor is efficient. It allows industry experts to do what they do best, namely to develop the standard of basic security practices. And it allows the control over improvements in security measures to rest with these industry experts. Enforcement follows industry–developed standards, rather than resting on static security requirements that are enshrined in statute or regulation.

Massachusetts has developed a way to rely on PCI DSS that is similar to the FTC's enforcement method. In its settlement with the Blair Group, it requires the company to maintain compliance with PCI DSS "or such compliance standards as may be from time to time recognized by the payment card industry as acceptable." [23] The difference between this recognition of the evolving nature of security standards and the static mandate contained in the Minnesota statute considered next could not be more stark.

A. STATE MANDATES

In contrast, the mandates such as the one embodied in a Minnesota statute are inefficient attempts to lock in current security practices into law. Minnesota's statute codifies the PCI requirement that security codes not be stored.[24] As discussed above, this element in the PCI standard is an important step in preventing the use of compromised information for the production of counterfeit payment cards. The security code is transmitted in a normal electronic request by a retail merchant for transaction authorization. If the code is

---

[23] Mass. v. Briar Group, LLC, Civ. No. 11-1185B, at 4, Consent Judgment (Mass. Sup. Ct. Mar. 28, 2011).

[24] Minn. Stat. § 325E.64(2) (2010). The statute is remarkably specific: "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."

missing or is the wrong code, this alerts the issuing bank to a problem and enables it to decline the transaction.

So why not just codify it? Part of the answer is that security standards are constantly evolving and what seems to be necessary today might be ineffective or counterproductive tomorrow. Industry experts are in a superior position to ensure that these standards keep up with changes in technology and the marketplace. Once those changes take place, a law such as the Minnesota statute creates a potential conflict between state law and the industry's best estimate of good security practices.[25]

Other dangers are more subtle and long-term. Once an element has become law, people tend to design systems around those requirements and do nothing else. But storage of security codes is only one danger. These codes can also be captured in transit, and other elements of the PCI standard speak to that danger. And the industry is looking at other measures such as encryption of data in transit to deal with that vulnerability. By codifying one element of industry practices but not others that currently exist or that might be developed, the law might be counterproductive by focusing efforts in some areas but sending the message that other measures are less important.

Moreover, if the state has mandated the use of one method, efforts to innovate to use different, but more effective methods are discouraged. Why spend the research and development resources to seek out and develop something new and better if the state would continue to require the older, less effective security measure? A similar point can be made about cost-effectiveness. If a new security measure accomplishes the same result at a fraction of the cost, why not use it and free up the resources saved for more productive uses? But the state mandate destroys the incentive for research and experimentation on more cost-effective security measures, since the old, more expensive approach would be required regardless.

These harmful effects are magnified by an aspect of the Minnesota statute that creates a new cause of action for entities harmed financially by a data breach. This cause of action is created when the entity whose system has been compromised has stored security codes in violation of the state's new security standard. [26] The beneficiaries of

---

[25] Governor Arnold Schwarzenegger used this argument in vetoing Assembly Bill 779, a California bill that would impose a security requirement similar to the Minnesota statute. *See* Letter from Arnold Schwarzenegger, Governor of California, to Members of the California State Assembly (Oct. 13, 2007), *available at* http://gov.ca.gov/pdf/press/2007bills/AB%20779%20Veto%20Message.pdf.

[26] Minn. Stat. § 325E.64(3) (2010).

this system are intended to be the financial institutions who, in reaction to a data compromise, expend resources to mitigate the harms that might result from the breach.[27] These actions typically include sending notification letters to their account holders, putting accounts on a watch list, canceling and re-issuing cards, and the losses resulting from fraudulent uses of the card. The idea is that financial institutions will be able to recover reasonable costs associated with these efforts from the merchants who have suffered a breach and have improperly stored security codes.

The industry has undertaken a process of allowing this kind of cost recovery. Under the older industry liability allocation rules, when a data breach occurred and fraud resulted, the liability for fraud losses and other expenses associated with the breach fell on the financial institution issuing the card. Other players were insulated. The cardholders themselves typically faced zero liability. The merchants where the fraud took place were normally paid in full and the banks provided service to these merchants, even though the transaction was not authorized by the actual cardholder.[28]

Most importantly, the merchants and processors where the data breach occurred, and the banks servicing them, were not held liable for the damages associated with the breach. As noted above, this created inefficiency and a disincentive to expend resources to keep cardholder information safe and secure. PCI was an attempt to remedy this inefficient alignment of incentives, by requiring compliance with industry standards as a contractual condition of being part of the payment system.

An additional effort on the part of the payment industry to correct this misalignment of incentives is to adopt an internal cost-recovery program. Under these programs, financial institutions that have been harmed by a data breach can use internal payment system process to recover some of the costs associated with the breach. The idea is to create a more balanced incentive structure, whereby merchants and processors who do not comply with industry security rules and cause harm to other payment system participants face financial consequences of their failure to follow good security practices. It is

---

[27] *Id.*

[28] The exception was for online merchants where, for a variety of reasons, liability for unauthorized use generally rested with the online merchant.

one way to move the industry to a higher level of compliance with PCI DSS.[29]

In contrast, legislated cost recovery programs are counterproductive. The control over the program shifts from private parties governed by their contractual obligations to the court system. Instead of rapid compensation for harms, the court process could simply create gridlock. Financial institutions could bring a case against a merchant firm who had suffered a breach alleging that it had improperly stored cardholder security codes. But the merchant could reasonably demand that the complainant prove to the court that it was responsible. The chain of causality between the alleged breach and the alleged harm has so many vulnerable links that this process could be easily extended indefinitely.

Consider the kinds of questions that could be asked. Was there really a breach? Forensic evidence is not always conclusive. If there was a breach, was it in the system under the control of the merchant, or did it occur at a different point in the transmission and storage of transaction information, perhaps at one of the upstream processors? If the breach was really in their systems, were they really storing security codes or did the hackers gain access to that information in transit? If they really were storing the security code and there really was a breach, was there any harm to the plaintiff from this breach? Often cardholder information is subject to multiple breaches and so it is a complex task to associate the harm with one breach with another breach or some other cause.

The steps that financial institutions can take to respond to a notification of a breach are within the discretion of the financial institution. Not all card numbers compromised in an alleged breach are actually used for fraudulent purposes. As a result, large financial institutions with substantial security and risk management departments and budgets can typically put the affected card numbers

---

[29] In the Visa system, this cost recovery program started in 2006 and was expanded in 2007. *See* Press Release, Visa, Visa Expands Fraud Recovery For Card Issuers (May 27, 2008), *available at* http://corporate.visa.com/media-center/press-releases/press780.jsp. Visa has also negotiated cost recovery settlements with breached entities that compensate to some degree the financial institution affected by a breach. *See* Press Release, Visa, 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 (Nov. 30, 2007), *available at* http://corporate.visa.com/media-center/press-releases/press748.jsp. In addition, there are financial penalties that can be assessed when a breached entity is out of compliance with PCI DSS. *See Cardholder Information Security Program*, VISA.COM, http://usa.visa.com/merchants/risk_management/cisp_overview.html (last visited Dec.12, 2011).

on a special watch list and see if there is any incremental fraud above the background rate. Smaller financial institutions, typically community banks and credit unions, usually react to a breach notice by immediately re-issuing cards. Is that a reasonable attempt to mitigate the possible damage from a breach? Once in a court context, there would need to be a court judgment about which financial institution responses were reasonable and which were excessively cautious. Financial institutions, thinking that they could recover all their costs from breached entities, might spend more than was necessary to protect their customers, and find themselves unable to recover these unnecessary costs in court.

All of these judgments would be referred to courts for decision. If other states imitate Minnesota then different courts might reach different decisions based on the details of the state level security standards imposed. Merchants in different states would face different standards of due care and financial institutions in different states would face different interpretations of their obligations to protect their consumers. These problems could be addressed through national legislation, but then federal courts would become the de facto interpreter of security requirements and duties of due care to financial consumers.

Merely listing these possible difficulties suggests that moving the questions of the right level of security to statute and to the court system is not likely to improve the level of security in the industry. Instead, it seems likely to result in interminable legal wrangles and to a work-to-rule mentality in the industry that could block further progress. [30] The problems are exacerbated when the prospect of litigation is used as an enforcement mechanism for a specific codified security standard. Companies facing limited resources for security investments will move to limit litigation risk by complying with just the elements called for by the statute.

A. ONLINE BANKING SECURITY

[30] These issues can of course arise in the private sector cost recovery programs operated by the payment networks, but they are less likely to result in gridlock. The goal of these programs is not to have aggrieved parties trying to extract the maximum amount from defendants in a legal proceeding, but to do rough justice that balances the interests of different parties in the same private payment system. Parties dissatisfied with the results can always pursue their rights in court. The success of these private sector cost recovery efforts is indicated by the fact that the overwhelming majority of financial institutions offered a settlement in the TJX case, accepted it and abandoned their efforts to recover costs through the court system. *See* Press release, Visa and TJX Agree, *supra* note 29.

There is an additional role for government when there is a widespread lapse in industry security practices that is exposing the industry collectively to harm. This occurs in the case of password-based single-factor authentication and phishing. When phishing attacks against financial institutions began to increase in number and sophistication in the early 2000s, an obvious security improvement was to introduce two-factor authentication. Phishing attacks were successful in part because customers were duped into revealing information at fake financial services sites that fraudsters could then use to gain access to financial accounts. For instance, when a customer divulges a password at a bogus financial services website, hackers can then use that information to gain access to his account at the real financial services website.

Two-factor authentication tries to avoid this problem by requiring that the customer have an additional factor – typically something the customer has in his possession – in addition to a password. This token generates a constantly changing password that is synchronized with the legitimate bank's website.

This security measure is by no means perfect. It is still vulnerable to "man in the middle" attacks. But it is clearly an improvement over the use of static passwords. The industry expenditures in moving toward this new system would be repaid by more than compensating reductions in fraud losses. In a market free of imperfections, industry participants would move toward this more efficient level of security.

In 2003, however, the industry was stuck and unable to move toward this new technology. The problem was that excessive security measures would increase customer dissatisfaction. The customer would be required to carry with him or have available a security token for each of his financial accounts. This customer inconvenience would make it likely that the first bank to impose a security requirement calling for an extra process and token would begin to lose customers to those banks who did not have this requirement. No one wanted to go first, and the industry was stuck in a situation of inadequate security with no market incentive to move from this inefficient position.

Financial regulators took action. They updated guidance for financial institutions related to authentication for online banking to require stronger authentication when high risk transactions are present. [31] The agencies could have simply mandated two-factor

---

[31] *See* FED. FIN. INST. EXAMINATION COUNCIL, AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT (2005), *available at* http://www.ffiec.gov/pdf/authentication_guidance.pdf.

authentication, with all the consumer inconvenience that would entail, and they did consider that alternative during the proposal stage of the process. But the final rule did not mandate two-factor authentication. Its conclusion was the more modest one; that passwords alone were no longer an adequate authentication strategy for online banking. Two-factor authentication or other compensating controls should be used in risky situations when transactions involve access to customer information or the movement of funds.[32]

This balanced approach allowed the industry to move from its inefficient equilibrium. Some institutions moved toward genuine two-factor authentication involving tokens. But others introduced other controls. A common one is the use of pictures and other identifying information that indicate to the customers that they are at the genuine financial institution's website. If they do not see this identifying symbol, they know that they are not at the right website and will refuse to divulge access information.

Other control mechanisms included the use of device authentication technologies that recognize the computer or other similar devices that customers are using to access the account. When an unfamiliar device attempts to access the account, the financial institution prompts for answers to a series of pre-arranged security questions. Even if the hacker has been able to obtain static password information from the customer, they would be unlikely to have this additional information as well. The use of additional security questions often takes place when customers are attempting to move funds through bill paying mechanisms or funds transfer to other accounts.

Other elements are clearly necessary to respond to the threat of phishing attacks. One is consumer education. Financial institutions regularly advise their customers that they will not ask for access information in a transaction that they initiate. This alerts customers that if they did not initiate a transaction, they should not divulge access information.

Measures to take down phishing sites are also important. The industry has cooperated with ISPs, webhosts, system administrators, domain name registrars and other Internet intermediaries to identify

---

[32] In 2006, FFIEC acknowledged that two-factor authentication was not required as long as some other method was used in addition to single factor authentication. BD. OF GOVERNORS OF THE FED. RESERVE SYS. ET AL., FREQUENTLY ASKED QUESTIONS ON FFIEC GUIDANCE ON AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT 2 (2006), *available at* http://www.fdic.gov/news/news/financial/2006/authentication_faq.pdf.

and take down suspected phishing sites rapidly.[33] Take down is accomplished in this context quickly and without any legal compulsion to do so. The weakness of the process appears to be the rapid rate of reappearance.[34]

The regulators had an effect on the industry not by mandating a particular technological response to the phishing problem, but by concluding that the industry's static single password authentication system was inadequate. The mandate to use multifactor authentication would have locked the industry into a particular type of technology and would have failed to allow the flexibility to tailor the security response to the nature of the risk and the extent of the possible financial harm. The conclusion that the status quo was unacceptable, on the other hand, forced the industry to innovate to meet the challenges of new regulatory expectations. Because the new guidance would be enforced through the examination process, financial institutions had to move beyond the inefficient status quo that had them unwilling to make security innovations for fear of losing customers. Because all of them were required to upgrade, the threat of customer migration to other financial institutions was mitigated. In effect, government had done what government does best: provide a coordinating mechanism to overcome a collective action problem.

In June 2011, FFIEC released a supplement[35] to its earlier guidance. In this supplement the FFIEC recommends that banks "offer" multifactor authentication to their business customers. This is a step beyond their previous view that two-factor authentication was not required when some other method of risk mitigation was used to supplement single-factor authentication. Notice that this recommendation does not encourage banks to require that their customers use multifactor authentication. But it is a clear strengthening of their earlier guidance and could be part of an evolution to a multifactor authentication requirement.

A. EUROPEAN SMART CARD PARTNERSHIP

---

[33] *See* Tyler Moore & Richard Clayton, *The Impact of Incentives on Notice and Take-down*, *in* MANAGING INFORMATION RISKS AND THE ECONOMICS OF SECURITY 199 (M. Eric Johnson ed., 2010).

[34] *Id.*

[35] *See* FED. FIN. INSTS. EXAMINATION COUNCIL, SUPPLEMENT TO AUTHENTICATION IN INTERNET BANKING (2011), *available at* http://images.avisian.com/Auth-ITS-Final_6-22-11_FFIEC_Formated.pdf.

Sometimes government can take a stronger role than merely concluding that the current level and direction of security controls are insufficient. They can, in addition, play the role of convener to nudge the industry along the path to a specific set of security controls or system architecture. This can happen when there is widespread agreement that the new controls or system architecture would be an improvement, but a government role can help to clear away institutional impediments. The example of the European transition to smart cards illustrates this type of government involvement.

Some background on chip and PIN (person identification number) technologies will help to set the stage for this discussion. The PIN part of the smart card security system is the requirement by the cardholder to input a PIN number as part of the authentication process. PIN-based debit cards, widely in use in the United States as access devices for ATM machines, illustrate this aspect of smart card security.

Smart cards systems also include a microprocessor to generate encrypted information and a point-of-sale terminal capable of generating and receiving this information. In a standard implementation, 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.[36] As a result, 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.

Objections to chip and PIN use have been made. Some argue that they are not secure and evidence of vulnerabilities has been produced. In addition, the liability shift associated with the move to chip and PIN has been criticized as unfair to cardholders who are now liable for unauthorized transactions that used to be the responsibility of financial institutions.

Whatever their validity, these objections relate to the PIN part of chip and PIN, and not to the chip part. The security vulnerabilities alleged have to do with the ability of hackers to complete chip and PIN

---

[36] 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 that is transmitted cannot be used to perform another contactless transaction or to create a counterfeit card.

transactions without knowing the PIN. Using a "man in the middle" attack researchers at Cambridge University were able to complete a valid transaction without entering the PIN.[37] This suggests that a PIN is not sufficient to protect against the use of a stolen card.

These alleged PIN vulnerabilities also suggest that cardholders should not be held liable for these unauthorized transactions. Banks in areas where chip and PIN have been implemented have not changed the basic standard of liability for unauthorized use. The current version of the banking code in the United Kingdom has a section on unauthorized use, which seems to preserve the immunity of cardholders from liability. [38] 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."[39]

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.[40] But if "man in the middle attacks" that allow the use of the card without the PIN are frequent enough, then this uniform assumption of gross negligence on the part of the cardholder is no longer justified.

One advantage of a chip card, however, has nothing to do with the use of the PIN to prevent the use of stolen cards. As Visa's Ellen Richey says,

> Visa has repeatedly underscored the need for authentication solutions to move to dynamic data technologies such as EMV chip . . . . [W]e believe the future of security lies in dynamic data. Our experience

---

[37] Steven J. Murdoch et al., *Chip and PIN is Broken,* 2010 IEEE SYMP. ON SEC. AND PRIVACY 433, 436 (2010), *available at* http://www.cl.cam.ac.uk/research/security/banking/nopin/oakland10chipbroken.pdf.

[38] LENDING STANDARD BD., THE LENDING CODE 16 (2009), *available at* http://www.lendingstandardsboard.org.uk/docs/lendingcode.pdf.

[39] *Id.*

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

> suggests that as markets move to chip they become less vulnerable to counterfeit fraud and, ultimately, to mass data compromise attacks.[41]

The key advantage of chip cards is that they generate dynamic authentication information. If the information used to complete one transaction is compromised, it cannot be used for another transaction. Each transaction needs new authentication information. As a result, the incentive to steal transaction information from storage or in transit evaporates. Even if the attack is successful, the information acquired is not useful for committing fraud.

This advantage of chip has nothing to do with the use of a PIN, so a demonstration that the use of a PIN is ineffective against stolen card fraud, even if valid, establishes nothing about its utility to prevent unauthorized use related to data compromises.

It is possible to take advantage of the chip feature of smart cards to reduce counterfeit fraud even if there is no PIN feature to reduce the incidence of stolen card fraud. Indeed, this is the case for the contactless chip cards introduced in the United States by Visa, MasterCard and American Express. They have dynamic data for authentication purposes, but do not require the use of a PIN. If someone steals a US-issued contactless card, it can be used for other transactions without the introduction of a PIN. Indeed, the use of a PIN with a contactless card would make them less easy to use and less convenient for consumers than current magnetic stripe cards. It would also not allow the increase in throughput at the cash register which is the major advantage of contactless cards for merchants.

So how did smart cards come to be widespread in Europe while they do not exist in large numbers in the United States? The answer lies in a private–public collaboration that managed the transition from magnetic stripe cards to smart cards.

In the late 1990s, the European banking regulators, European Commission officials and the banking industry together began to move toward the implementation of chip and PIN. In 2001, the European Commission 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

---

[41] Press Release, Visa, Visa Program Encourages Merchant Adoption of AMV Chip as Path Toward Dynamic Authentication (Feb. 9, 2011), *available at* http://corporate.visa.com/media-center/press-releases/press1098.jsp.

> 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.[42]

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.[43]

In 2004, the Commission issued a further action plan.[44] It reported a decline in the growth of card fraud from 50% per year in 2000 to 15-20% in 2004, attributable to the increased efforts of the payment industry and national authorities in implementing fraud reduction measures.[45] 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.

---

[42] *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*, at 3, COM (2001) 11 final (Feb. 9, 2001), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0011:FIN:EN:PDF.

[43] *Id.* at 5, 10 n.11.

[44] *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*, COM (2004) 679 final (Oct. 20, 2004), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0679:FIN:EN:PDF.

[45] *Id.* at 3 n.5.

> The Commission and national authorities should be prepared to assist the migration to chip cards in the EU, if necessary.[46]

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 EU Fraud Prevention Expert Group (FPEG) of the European Payment Council. [47] 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."[48]

The move to chip and PIN was also part of the movement to set up a European payment area. In its 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."[49] In its 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.[50]

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 provided an incentive to move all terminals and all cards toward compliance with chip and PIN. The liability for fraudulent transactions passed to the

---

[46] *Id.* at 5.

[47] *Id.* at 3.

[48] *Id.* at 4 n.8.

[49] *Annual Progress Report on the State of SEPA Migration in 2008*, at 15 (2008) [hereinafter *State of SEPA Migration*], *available at* http://ec.europa.eu/internal_market/payments/docs/sepa/progress_report_2008_en.pdf.

[50] *Second Annual Progress Report on the State of SEPA Migration in 2009*, at 10 (Nov. 9, 2009) [hereinafter *Progress Report*], *available at* http://ec.europa.eu/internal_market/payments/docs/sepa/progress_report_2009_en.pdf.

party that is not EMV-compliant in the case of lost, stolen, or counterfeit cards.[51] While not mandated by public authorities, this liability shift had the tacit support of public authorities as an effective method of achieving the goal of transitioning to a chip and PIN system.

The concerted effort was successful. Europe moved to the new liability regime on January 1, 2005.[52] So did the United Kingdom.[53] 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.[54] 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.[55]

It is reasonable to wonder whether the same public-private partnership could work in the United States. It might not. The relationship between government and business is more adversarial in the United States than in other countries. Financial regulators have had, in part, the responsibility to protect the safety and soundness of individual institutions and the stability of the industry as a whole. But they have tended to defer to industry in their day-to-day practices when safety and soundness or stability is not at issue. So, some skepticism might be in order in connection with US regulators playing the same convening role that European regulators did so successfully in the case of smart cards.

One feature of the situation holds out some hope for action in this area. Financial regulators can have acted successfully to ameliorate collective action problems in the area of information security. As we have seen, their regulatory "nudge" moved the industry beyond single

---

[51] *See* CAPGEMINI & ABN AMRO, WORLD PAYMENTS REPORT 2006 26 (2006).

[52] Robin Arnfield, *Here Comes EMV*, CREDIT CARD MGMT., Jan. 3, 2005, http://search.proquest.com/docview/201146993/fulltextPDF/13207C6F31066640614/1?accountid=9783. The Visa chip mandate schedule is part of its International Operating Regulations. *See* VISA, VISA INTERNATIONAL OPERATING REGULATIONS SUMMARY OF CHANGES (2011), *available at* http://usa.visa.com/download/merchants/visa-international-operating-regulations-summary.pdf.

[53] *See Shift of Liability for Fraudulent Transactions*, CHIP AND PIN, *available at* http://www.chipandpin.co.uk/business/card_payments/means/shift_liability.html (last visited Feb. 29, 2012).

[54] *State of SEPA Migration*, *supra* note 49, at 15.

[55] *Progress Report*, *supra* note 50, at 10.

factor authentication. It is true that they would have to be more affirmative in their direction to the industry in the case of smart card introduction in the U.S. They would not simply be able to say that the static authentication embodied in magnetic stripe cards and terminal readers was unacceptable. They would have to affirmatively take steps to encourage the industry adoption of the dynamic authentication embodied in smartcards. The industry might not be resistant to that as has been indicated by recent statements from industry leaders. The institutional blockage is less whether the new technology is effective and worth it for the industry as a whole. The real obstacle appears to be appropriate sharing of the costs and benefits of the transition. With good will and cooperation from all parts of the industry, regulators might very well be able to assist the transition to a higher and more efficient level of security.

III. PART THREE

A. LESSONS LEARNED

In this section, I sum up some of the lessons that can be learned from the examples just described. The overall theme is that no one way of government interaction with the private sector is the one, exclusive right way to do things. It depends on the nature of the objective to be achieved and the obstacles that have to be overcome.

Another overall theme is the need to be clear about the goal to be aimed at through combined industry-government action. At what level of security are we aiming? It is a commonplace that perfect security is a chimera. So what is the goal?

It might seem that a good starting point is that the right level and type of security investment by the financial sector is the level and direction for which a business case can be made by each financial institution looking at the costs and benefits to it. Independent actors assess the situation, and the aggregate result of these assessments filtered through the normal market forces will produce the best level of security.

But this is wrong for two reasons. First, the financial services world is an interconnected system. Vulnerabilities at one point affect other nodes in the system. This creates interdependency between the decisions that one party makes and the consequences for other parties. It might not be worth it to one party to make investments in security because the consequences of not making those investments fall on other parties. Second, existing liability rules, either contractual or legal, interact with these system vulnerabilities in ways that can

predictably generate underinvestment in security. Some participants have a classic free-rider incentive to under-invest in security because part of the benefit of their investment will accrue to others. This leads to underinvestment in security compared to what would be socially optimal. The notion of underinvestment here is not based on government substituting its judgment of the right level of security for the judgment of the private sector. The notion is the standard cost-benefit concept that the sum of the welfare of the parties affected would be higher if the amount of investment was higher or its direction was different.

So the goal is to make sure that the industry achieves this efficient level of security investment, taking into account the existence of misaligned financial incentives and security externalities that prevent individual business calculations from automatically producing this result. [56] I turn now to the lessons learned.

A. LIABILITY RULES AND REGULATORY RESPONSIBILITY

Government can have an extraordinarily powerful effect on the nature and size of security investments through the establishment of liability rules and regulatory responsibility. The example already discussed that illustrates this theme is the decision by the U.S Congress to limit the payment liability of cardholders for unauthorized use of their cards.[57] This decision to largely hold the

---

[56] Something like this Kaldor-Hicks principle is espoused in the "Greatest Good" principle included in the cyberspace proposal adopted by a coalition of business groups and civil liberties groups. *See* BUS. SOFTWARE ALLIANCE ET AL., IMPROVING OUR NATION'S CYBERSECURITY THROUGH THE PUBLIC-PRIVATE PARTNERSHIP: A WHITE PAPER 7 (2011), *available at* http://www.cdt.org/files/pdfs/20110308_cbyersec_paper.pdf.

[57] Banking regulators can shift liability in order to provide an incentive to control fraud to the party best positioned to take effective steps to achieve that goal. For instance, in 2005, in response to concerns about unauthorized remotely created checks, which are created by the payee and do not bear the account holder's signature, the Federal Reserve Board assigned liability for losses associated with unauthorized remotely created checks to the depositary bank that works with the payee. The idea was that in the absence of a signature the account holder's bank would have no way of knowing whether the check was legitimate. However, the depositary bank could monitor its customers to ensure that there were good business practices and could detect problems through monitoring the extent of returned items. The Board concluded that by shifting the liability for fraudulent remotely created checks it would "create an economic incentive for depository banks to perform the requisite due diligence on their [remotely created check] customers." *See* Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire and Availability of Funds and Collections of Checks, 70 Fed. Reg. 10509 at 10510, (proposed Mar. 4, 2005) (to be codified at 12 C.F.R. §§ 210, 229).

cardholders harmless meant that the costs of unauthorized use of payment cards fell on the financial institutions that issued the cards and the payment systems that processed the transactions. This financial impact drove the payment systems forward on a search for ways to minimize fraud losses from unauthorized use. Digitizing the transaction records had speed and efficiency factors that motivated its introduction, but it also enabled the use of computer and software mechanisms to control fraud. Two examples of these security measures were the use of card security codes embedded on the magnetic stripe and on the face or back of the cards themselves, and the use of neural networks to detect unusual patters of card usage. As a result, fraud levels in the payment card world have experienced a long-term secular decline since the 1990s. This decline has stopped and fraud rates in the industry have stabilized at about six cents for every 100 dollars worth of transactions.[58]

This decision to immunize cardholders from liability incentivized the financial system to take the necessary steps to improve security over time. The objective was not static, but was dynamic. The aim was not to get the highest level of security using whatever system architecture and safety precautions existed at the time. At the time the liability legislation was passed, the payment system was entirely paper and fraud was substantially higher than it is today. The immunity provision worked to upgrade the entire system.

The key lesson that policy makers can learn from this example is to pay attention to which party in the system has the ability to make system improvements to provide a higher level of security. In some circumstances, the ability to innovate to provide improvements rests at the edges of complex systems. One of the reasons the Internet has been so successful as an engine of innovation is that it distributes the ability to innovate to the edges of its networks, rather than centralizing this ability in the hands of the network operators. But not all systems have this end-to-end architecture. Financial systems in general and payment systems in particular tend to be centralized with decisions on system upgrades and changes in architecture made by the major industry players and network operators. Individuals at the edges of the system have almost no ability to bring about systemic changes, and therefore no ability to innovate to improve the level of security in the system.

One could argue, and many in the industry did argue, that individual responsibility for unauthorized use would provide an

---

[58] Press Release, Visa, *supra* note 15.

incentive to the cardholders to be careful with their payment cards. But this might at best help to control lost and stolen fraud, which was not and is not the major category of fraud loss. For counterfeit fraud, which is a major category, there is nothing individuals can do to reduce losses. When a hacker breaks into a merchant database and obtains millions of card account numbers, there is no basis for thinking that any level of individual cardholder diligence can prevent these cards from subsequently being used for fraudulent purposes.

This pattern of thinking should apply to current allocations of responsibility for providing reasonable levels of security. The thinking behind the PCI DSS and the use of this standard as an enforcement standard is based on the idea that the merchant or processor has the capacity to control information at their own site. But that is a static perception of the situation. There is a security vulnerability when the payment systems distribute key cardholder authentication information to the millions of merchants, processors and financial institutions in the system and then expect them all to provide the highest levels of security to prevent hackers from getting access to this valuable information. An architectural change that devalues this authentication information is clearly the most desirable solution.

There is nothing, however, that the merchants and processors can do on their own at the edges of the system to improve the architecture. A movement to chip and PIN for example is not something they can just voluntarily adopt. It has to be something done by the financial institutions and network operators who control the payment system architecture. As we have seen in the example of the European movement to smart card technology, all players in that system need to be involved in making the upgrade, and allocation of liability can be a useful tool to manage the transition.

A. REGULATION AND LEGISLATION

The lesson to be learned from our examples in the area of regulation and legislation is that these tools of government should be at the level of principles, with implementation left flexibly to the interaction of industry and government agencies. Government involvement is counterproductive when it locks specific security practices into law or regulation. In this regard, legislation such as Gramm-Leach-Bliley, which requires firms to establish appropriate processes to focus attention and resources on information security, is

appropriate.[59] Also appropriate would be requirements for reasonable security measures.[60]

The enforcement of a reasonable security requirement presents complex difficulties. Individuals and institutions could enforce the security requirements themselves through court actions. A private right of action might seem efficient since it distributes the enforcement burden from government agencies with limited resources to private parties who might have been harmed by security vulnerabilities. But this is a recipe for endless delay and even abuse. It ultimately means that courts will be determining what security practices are reasonable. While it is reasonable to expect that a regulatory agency assigned the task of enforcing security standards would develop some understanding of security issues, it is very unlikely that courts would be able to develop this expertise.

The best course of action for the enforcement of a reasonable security requirement would be at a national regulatory agency. In the financial sector, this means the functional financial services regulators for traditional financial institutions and the FTC for non-traditional financial institutions. The financial regulators are able to effectively carry out this responsibility as part of their ongoing examination responsibility. The FTC relies on complaints and orders to make sure that their rules are well understood and widely known. The recent financial services reform legislation did not disturb this allocation of responsibilities for security regulation in the financial services sector.[61]

A. CONVENER ROLE

---

[59] *See* 15 U.S.C. § 6801(b).

[60] Press Release, U.S. Senator John Kerry, Kerry, McCain Introduce Commercial Privacy: Bi-Partisan Legislation Would Enhance Protection and Control of Personal Information (Apr. 12, 2011), *available at* http://kerry.senate.gov/press/release/?id=59a56001-5430-4b6d-b476-460040de027b. The draft privacy legislation from Senator Kerry calls for the Federal Trade Commission to establish and enforce such reasonable security requirements. Previous privacy legislation and data breach notification legislation contained similar reasonable security requirements.

[61] Wall Street Reform and Consumer Protection Act H.R. 4173, as enrolled and passed by Congress (Pub. L.111-203). Title X establishes a new Consumer Financial Protection Bureau, which is given the responsibility for privacy regulation in the financial services sector. Responsibility for security, however, stays with the traditional financial service regulators and the FTC.

Government has a key role in identifying and eliminating coordination difficulties that prevent autonomous industry action. This can often be done by bringing the parties together to move them toward common action despite institutional blockages and misaligned financial incentives that impede this action. In the current case, these institutional roadblocks will be less about the efficient level of security investments and more about the allocation of costs and benefits associated with moving to a higher level of security.

The European transition to smart cards illustrates this role. In the United States there is an opportunity for public private partnerships to play a similar role. The industry seems to have converged on the idea of chip cards as a new architecture that will have substantial advantages. It is no longer a question of whether, but of when.[62] Visa has announced, for example, that it will provide some relief from compliance with PCI standards for merchants who have implemented chip and PIN. Unfortunately, because of regulations regarding interchange on debit cards, they have not moved to extend this trade-off to merchants in the United States.[63]

Government involvement in this transition would be helpful. The major issue is not whether this would be an improvement. Studies indicate that chip would have a payback period of approximately five years in terms of fraud reduction. But it is expensive to implement, approximately $13 billion. Each party in the system has to make upgrades in order for the system to accommodate chip cards. But each party does not benefit the same from the upgrades. Merchants and processors have to make the most substantial investments, but the financial institutions that issue cards would benefit the most. [64]

In this context, a government role to help allocate costs would be sensible.[65] Regulators are already heavily involved in the setting of interchange rates for debit cards. These interchange rates would be

---

[62] *See* Richey, *supra* note 15.

[63] Press Release, Visa, *supra* note 15.

[64] *Card Industry Has a Compelling Case for Data Encryption, Report Says*, BRIGHTERION.COM (Jan. 13, 2010), http://www.brighterion.com/PDFArticles/CardIndustryHasaCompellingCaseforDataEncryption.pdf.

[65] A cost allocation role associated with a government mandate is typical. See, for example, the British Government's decision to require ISPs to pay only 25% of the costs of its mandated graduated response law to control online copyright infringement. Digital Economy Act, 2010, c.24, § 15 (U.K.).

one possible way that the system could redistribute costs associated with upgrading the system. The card networks have used an interchange shift to provide an incentive to move to chip in other jurisdictions.[66] With appropriate non-regulatory encouragement from the government, a similar incentive interchange structure could provide reasonable cost sharing that could motivate all parties to make the transition.

Existing institutions can mediate these conversations. The FS-ISAC[67] is one such entity. It has wide industry membership including American Express, Bank of America, Citigroup, Fannie Mae, Morgan Stanley, Goldman Sachs, JP Morgan Chase, PayPal, and Wells Fargo and participation from government entities as well including The Federal Reserve and Federal Reserve Bank of New York. It gathers information about cybersecurity threats and vulnerabilities from various sources and distributes it back to its member organizations. It also provides recommended solutions from industry experts.

The U.S. Department of the Treasury, the Office of the Comptroller of Currency, the Department of Homeland Security (DHS), the United States Secret Service, and the Financial Services Sector Coordinating Council recommend FS-ISAC membership. In fact, both Treasury and DHS rely on the FS-ISAC to disseminate critical information to the financial services sector in times of crisis.

Another useful intermediary organization for public-private cooperation in this area is the Financial Industry Sector Coordinating Council.[68] The Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC), established in 2002, is the sector coordinator for Financial Services

---

[66] Vidyalaxmi & Preeti R Iyer, *Visa, MasterCard Want Banks to Pursue EMV Technology*, BUS. STANDARD (Jan. 17, 2006), http://www.business-standard.com/india/news/visa-mastercard-want-banks-to-pursue-emv-technology/234665. For MasterCard's interchange shift, see *Regional Liability Shift Policies*, MASTERCARD ONLINE, https://mol.mastercard.net/mol/molbe/public/login/ebusiness/smart_cards/one_smart_card/chip_migration_strategy/liability_shift.jsp (last visited Feb. 29, 2012).

[67] *See* FIN. SERV. INFO. SHARING AND ANALYSIS CTR., http://www.fsisac.com (last visited Feb. 29, 2012) (stating that the Financial Service Information Sharing and Analysis Center is an "industry forum for collaboration on critical security threats facing the financial services sector.").

[68] *See* FIN. SERVS. SECTOR COORDINATING COUNCIL, https://www.fsscc.org/fsscc (last visited Feb. 29, 2012) (stating that 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.").

for the protection of critical infrastructure, focused on operational risks. Because the FSSCC fits into a larger network of industry/sector coordinating councils, it is uniquely positioned as the leader within financial services for developing strategies to improve shared critical infrastructure and homeland security.

The FSSCC's mission is further supported by Homeland Security Presidential Directive #7, which directs government agencies to identify and protect critical infrastructure. The FSSCC works closely with the Treasury as its designated Sector Specific Agency (SSA), establishing a strong public-private partnership to maintain a robust sector that is resilient against manmade or natural incidents. Members commit their time and resources to FSSCC with a sense of responsibility to their individual firms and for the benefit of consumers and the country's populace.

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.[69] BITS is also an organization that could aggregate and organize industry expertise.[70] The missing piece for these organizations is explicit involvement from government.

A. RANGE OF GOVERNMENT ROLES

The most important lesson is for policy makers to examine the entire range of possible involvement and pick the right tool for the

---

[69] Press Release, PCI Security Standards Council, PCI SCC Collaborates with a Variety of Stakeholders in Determining When to Upgrade PCI DSS (Nov. 16, 2009).

[70] *See* BITS, http://www.bitsinfo.org (last visited Jan. 29, 2012). BITS is an industry consortium made up of 100 of the largest financial institutions in the US and associated with the Financial Services Roundtable. It "provides intellectual capital and fosters collaboration to address emerging issues where financial services, technology, and commerce intersect." *Id.*

right job. The legitimate government role lies along a range from low to high involvement:

- Industry autonomously evolves security standards;
- An enforcement role putting the weight of government behind industry-developed and upgraded standards;
- More active phase where government agencies conclude that current industry practices are inadequate and must be improved but does not mandate or promote any particular solution; and
- A still more active phase where government actively encourages industry to adopt a particular security approach.

When industry is beginning to develop a solution to a problem, the first stage of industry autonomy might be the most appropriate. This is what happened as the payment card industry began to develop the PCI DSS. It was first perceived as an industry problem. The existing financial incentives were inadequate to encourage merchants to safeguard cardholder information and so the industry began to develop a non-regulatory, private standard, to be enforced through the web of contracts that knits the payment systems together.

When enforcement of these standards purely by industry efforts seemed to be flagging, the government role properly shifted to one of bringing to bear government sanctions against entities that did not comply with the standard. The mechanism chosen was not lawsuits by private parties, but rather enforcement action by a regulatory agency, the Federal Trade Commission. Once the industry had developed the security standard, the regulatory agency could view the standard as a measure of what was reasonable for companies to provide. No one could expect the regulatory agency to have the expertise to create or require upgrades to the standard, but they could reasonably defer to the industry standard as a standard of due care. And over time, they could develop an expertise in understanding how the standard was interpreted, validated and enforced.

A more active stage can be reached when the industry seems stuck in a level of security activity that fails to take advantage of clear, well-

understood security steps that would pass a cost-benefit test if they could be implemented. This took place in the case of the federal regulators' reactions to the phishing problem for online banking. A collective action problem prevented each financial institution from moving on its own, but with the decision that the status quo of password-based single factor authentication represented inadequate levels of security, the industry could move collectively to a higher stage of security. Notice at this stage, however, the government did not mandate or nudge the industry toward any particular technology as the solution.

A final stage takes place when a new system architecture or security solution appears to have well-documented advantages, but industry players are not moving or cannot move toward that solution. The government role here is to act as a convener to overcome institutional obstacles. The movement to chip in the European Union illustrates this role. In the United States, a similar role would makes sense to overcome the distributional concerns that appear to be blocking the move to chip technology, despite a general understanding that this would represent a cost effective solution if the industry could get there.

It is possible for government to go beyond that by mandating specific security measures as a matter of law or regulation. In general, however, the government should refrain from enshrining specific security measures in law or regulation, since this can freeze innovation, lock in less effective security measures and prevent the development of compensating controls that are less costly and equally effective.

IV. CONCLUSION

The key role for government is to keep an eye on the system and not on any of the individual participants. Its aim is not to encourage more security for the sake of more security, but to make sure that desirable upgrades, improvements and innovations are made.

It is important to emphasize that this notion of desirable upgrade that should be the basis for government involvement is not that security is good and more security is better. There is a limit to what needs to be spent on security. If too much is spent on security, then the consequences for people will be negative. We will lose value in our financial services and products when we pay more for security than can be recovered in reduced costs.

There is a wider issue here, however, which should be mentioned, even though I do not have much to contribute to its solution.

Sometimes the damage that can be done through vulnerabilities in the financial services sector falls on organizations and institutions outside the sector. Disruptions of the financial system or the payment system can affect people in all aspects of their lives and lead to delays and shortages in other parts of the economy. Gains from stolen payment card information can be appropriated by terrorist organizations and used to inflict physical damage and other harms on other sectors.

These external effects are beyond the capacity of financial services regulators and the financial industry to address on their own. There might be a need to move the industry to a higher level of security to compensate for these extra-systemic effects. This needs to involve wider coordination with larger industry and governmental groups. The coordination efforts described at the beginning of this article by the FSSCC are part of this wider government-industry effort. The Administration's expected cybersecurity proposal might provide direction in how to move in this direction.

It is possible that government policymakers and other industry officials think that extra security needs to be provided in the financial services sector beyond what would be justified by an analysis of the internal costs of security flaws to industry participants. If so there might need to be a government role to provide an incentive for the financial sector to make these additional expenditures.[71]

This paper has identified a range of roles for government to play to promote socially beneficial security measures in the financial services sector. They each have their advantages in particular contexts. The choice should be made depending on the details of the particular situation, rather than on some overarching conception of the right role for government to play. Cooperation and coordination are the good words in this context. With these flexible ideals as our guide, industry and government can together move the industry toward a higher and more socially beneficial level of security.

---

[71] *See* Bus. Software Alliance et al., *supra* note 56, at 7.