



Shift4[®]

Secure Payment Processing

Information Security in the Payment Process

Compliance Versus Security

Authored by Dr. Heather Mark, Ph.D., CISSP

February 2006

Executive summary

“Information Security” has become a growing concern for all businesses. In the Payment Services Industry, in particular, the security of customer information has taken on extreme importance. Yet despite all the attention it garners, there is still a great deal of confusion about the concept. Many businesses approach information security by implementing only those measures that are required for compliance with the Payment Card Industry Data Security Standard (PCI). The popular misconception holds that a company that is compliant with the PCI standards must also inherently be secure. Such an approach may be shortsighted and not adequate to sufficiently protect the company’s sensitive information and computer resources. This paper will define information security and contrast the definition with that of compliance. A discussion of the Card Association data security programs, the Payment Card Industry Data Security Standards and the Payment Application Best Practices, will be included. The difference between the concepts of information security and compliance will be illustrated. Following that, the importance of good security practices will be presented.

Disclaimer

The information provided herein is for informational purposes only. This paper is not meant as compliance advice. Prior to taking any steps that may affect your compliance status with industry or government mandates always seek advice from your compliance auditor and/or legal counsel.

Introduction

Information security is a fairly new term in the world of business. Though the phrase first manifested itself in the early 1960s, it was thought of largely in terms of physically securing the computer equipment itself. With the advent of remote access technologies in the late 1960s and early 1970s, the concept of information security took on new meaning. In 1967, the Department of Defense released a report entitled, “Security Controls for Computer Systems.” It was re-issued in 1975, yet information security still remained in the realm of the subject matter experts and was not a common concern for businesses or individuals. It was not until the late 1980s and early 1990s that personal computers began to gain the popularity that they enjoy today. This brought to light a whole new focus on the protection of information. Though the practice and discussion of information security has been common since the 1990s, the Payment Services Industry is a relative neophyte in the adoption of information security practices.

Though identity theft is the fastest growing crime in the world, the industry was slow to react. The lack of movement towards standardizing information security practices in the Payment Services Industry can be compared to the lack of regulation of the meat packing industry before the damaging expose, *The Jungle*, published in the early 1900s by Upton Sinclair. The Food and Drug Administration was brought about by Sinclair’s scathing account of the meat packing industry published. This brief history lesson is offered to illustrate a pattern in U.S. policymaking of waiting until after disaster strikes to take action. There is a basic theory of public policy that states that government action is driven by crisis. The same theory is at work at the industry level.

Armed with that knowledge, it should come as no surprise that the Payment Services Industry was reluctant, at best,

STORING CREDIT CARD DATA

to embark on the project of establishing a baseline of information security. Although it was common knowledge that the industry was predicated upon the collection, storage and transmission of sensitive information, there was no consensus as to the risk that was posed to that information. Though Visa USA and MasterCard had both adopted information security programs in 2001, the adoption had been slow and enforcement was sporadic. Until 2003, there had yet to occur an event that galvanized the industry into action. The industry stakeholders had been able to continue their business under the assumption that there was no need to enact the sometimes expensive protections required to reduce risk to personal information. That complacency was shaken in 2003, when a small processor unknown to the major card associations was compromised, resulting in the exposure of over 13 million credit card account numbers.

The DPI breach of February 2003 revealed some startling vulnerabilities in the Payment Services Industry. Not only were the associations unfamiliar with the fact that DPI existed, much less that the company was processing credit cards, the sheer magnitude of the breach was of particular concern. At the time, it was the largest breach in U.S. history. Additionally, the breach garnered much more media attention than any previous incident. The brand damage associated with the loss of the account numbers, in addition to the fiscal burden of replacing compromised cards, served to spur the card associations to take a more proactive role in enforcing their data security programs.

Since 2003, information security has become a much more pressing concern to those in the Payment Services Industry. Data security has become a major topic at industry events. All of the major publications servicing the industry have devoted columns and articles to the issues surrounding the protection of sensitive information.

Companies have become more proactive in the adoption of strong information security principles. Information security has increasingly become a competitive advantage. Despite these efforts, however, the frequency and magnitude of data security compromises has increased.

In 2005, there were over 130 compromises that resulted in the exposure of over 50 million account numbers. The growth in the number of compromises was accompanied by a shift in the target of the compromises. Historically, the processors and other services providers had been the targets of the attacks. Supposition is that these targets provided a “bigger payoff” for the intruders, since they housed thousands, sometimes millions, of account numbers. As these companies became increasingly secure, and likely because of the attention focused on their security by the card associations, the attacks shifted to retailers and have become more high profile. As the breaches continue to grow in number and size, the media and the government are becoming increasingly involved in the data security posture of the Payment Services Industry.

Increased role of regulation in the payment service industry

The Payment Services Industry in particular has come under increased scrutiny in regards to the protection of non-public personal information. Over the last years, a number of well known retailers and large processors have been the victims of security breaches resulting in the loss of millions of credit card numbers. Sam's Club, the latest to announce a breach (12/05), did not specify the number of cards stolen, but the effect has been to re-energize the attention already focused on the industry largely as a result of the CSSI breach in early 2005.

In February of 2005, Card Systems Services International announced that they had lost credit card data. This was especially significant as the company was listed as a PCI compliant company. Even more startling was the number of card numbers that had been exposed: over 40 million. Upon further investigation, it was discovered that the company was grossly out of compliance with the PCI at the time of the compromise. The result was that Visa and American Express revoked the company's ability to process their cards. In the aftermath of the compromise, Congress called for special hearings on data security in the industry.

The sheer magnitude of the losses is enough to garner attention from the regulatory bodies of the U.S. government. In 2005, both Visa USA and MasterCard testified before Congress regarding the state of security in the industry. In both cases, the associations urged Congress to pass far-reaching data security bills. Joshua Peirez, Senior Vice President and General Counsel for MasterCard stated "that the law should establish clear data protection requirements for entities in possession of sensitive personal information if such entities are not

already covered under the Gramm-Leach-Bliley Act¹." Representatives from Discover and American Express also testified at the hearings.

The Federal Trade Commission (FTC) has also taken an increasing interest in the protection of personal data in the credit card industry. Part of this interest derives from the FTC's authority under the Gramm-Leach-Bliley Act (GLBA), which provides the commission with the ability to enforce the Privacy and Safeguard Rules of the GLBA. In essence, these provisions of the GLBA require companies to enact certain procedures and protections around personal information to prevent unauthorized disclosure. FTC authority also derives from §5A of the Federal Trade Commission Act. This provision of the act gives the Commission the authority to prevent deceptive and unfair trade practices. The authority granted under the provision has been broadened to the point that the FTC can prosecute companies for failing to enforce their own privacy policies.

The increased awareness comes as no surprise to seasoned information security professionals, who have long championed the cause. There is, however, still quite a distance to close between being aware of information security and truly understanding it. In today's business environment it is often difficult to avoid the term "information security." Its use has become ubiquitous. From boardrooms to the halls of Congress, information security and its assurance are common topics of conversation. Poor information security and its implications for the economy and even national security render the protection of sensitive information a top priority in business and in government.

¹ Peirez, Joshua L. "Credit Card Processing: How Secure Is It? Testimony of Joshua L. Peirez, Senior Vice President and General Counsel MasterCard International." Available online at (<http://financialservices.house.gov/hearings.asp?formmode=detail&hearing=407&comm=4>)

Payment service industry data security

The federal and state regulators were not the only entities that grew increasingly concerned over the protection of non-public personal information. The card associations were also concerned. Naturally there was concern over the incidents of fraud that are generally foretold by such a data compromise. Inherent costs, such as notification to consumers, reissuing of cards, and fraud liability are a grave concern to the associations. In addition, however, the associations were, and remain, mindful of the brand damage that occurs when credit card data is lost or stolen. Perhaps equally important, however, was the desire to appear proactive to federal regulators. To address these concerns the card associations began to develop data security programs.

Payment Card Industry Data Security Standard

In 2000, both Visa USA and MasterCard International introduced data security programs: the Cardholder Information Security Program and the Site Data Protection program, respectively. The two programs established a baseline of security measures that must be taken by companies that were handling cardholder data. Compliance with the programs was mandatory, however adoption of the programs in the industry was quite slow. Both American Express and Discover also introduced data security programs, though compliance was not compulsory. Rather than increasing the level of data security in the industry, the existence of four disparate programs made companies reluctant to move forward with their compliance projects. This was exemplified by the DPI breach in 2003, which resulted in the compromise of over 13 million card numbers. Recognizing that the existence of four data security programs could be counterproductive, the card associations began to collaborate on the creation of single, all-encompassing data security standard for the Industry. In January 2005, the associations introduced

the Payment Card Industry Data Security Standards, also called the PCI.

The PCI consists of a set of high level objectives designed to increase the security posture of the industry as a whole.

Those objectives are:

1. Build and Maintain a Secure Network
2. Protect Cardholder Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

Each of these objectives is supported by a number of requirements and sub-requirements that detail the way in which each objective is to be met.

The PCI draws heavily from Visa USA's CISP. The objectives and format of the requirements are strikingly similar. Brevity precludes a lengthy recitation of the requirements here, but a copy of the PCI can be obtained at the websites of the four major card associations. All companies that store, transmit, process, or otherwise handle cardholder data are required to comply with the PCI requirements. The method by which companies must validate compliance varies according to the volume of transactions. The card associations have delineated the industry by the type of company (merchant, processor, etc.) and the size of the company (number of transactions processed annually), and created validation requirements commensurate with those categorizations.

Visa and MasterCard have established the following guidelines:

Service Provider	Level 1	All VistaNet Processors, all Gateways
	Level 2	Over 1 million transactions annually
	Level 3	Less than 1 million transactions annually
Merchant	Level 1	More than 6 million transactions per card brand
	Level 2	Between 150,000 and 6 million transactions annually
	Level 3	Between 20,000 and 150,000 transactions annually
	Level 4	Less than 20,000 transactions annually

It should be noted that, according to MasterCard, all registered Third Parties are automatically considered to be a Level 1 Service Provider. A third party provider is defined by MasterCard as a company that processes or handles data on behalf of a member or merchant. Additionally, the card associations have mutually agreed that the company in question must meet the validation criteria of the highest level in which they are categorized by any given card brand. For example, if a merchant processes 6 million Visa transactions, they would be considered a Level 1 merchant by Visa. Even if that company processes only 5 million transactions for MasterCard, that merchant must still validate compliance in the manner prescribed for Level 1 merchants. American Express and Discover have much lower transaction rates than Visa and MasterCard. For that reason, their leveling is somewhat different than that described above.

The leveling described above does not have any impact on compliance. All companies, regardless of business model or transaction volume must comply with the PCI

requirements. There are no exceptions.

Service Provider	Level 1	Annual on-site assessment and quarterly network scans
	Level 2	Annual on-site assessment and quarterly network scans
	Level 3	Annual self-assessment questionnaire and quarterly network scans
Merchant	Level 1	Annual on-site assessment and quarterly network scans
	Level 2	Annual self-assessment questionnaire and quarterly network scans
	Level 3	Annual self-assessment questionnaire and quarterly network scans
	Level 4	Recommended annual self-assessment questionnaire and quarterly network scans

While it is only recommended that Level 4 merchants perform the validation procedures outlined above, all merchants are still required to comply. Those that do not comply are subject to fines and penalties. Companies that suffer a breach and are found to be non-compliant at the time can be subjected to fines of up to \$500,000. Additional fines can be levied for those companies that fail to report a suspected breach. In the worst cases, those in which the company is egregiously out of compliance, the card associations may impose the “death penalty,” refusing to accept any further transactions from the company.

Payment application best practices

With the data security programs established, it would seem that the instances of data loss would be on the decline. Unfortunately, the Payment Services Industry had fallen victim to a new trend: the use of the application as the route to unauthorized disclosure of credit card information. Companies that were compliant with the data security programs were being breached through the application used to accept credit card payments. The industry needed to take action to mitigate the attacks that were occurring through the payment application.

One of the most common breaches seen is the SQL injection attack. Perhaps most familiar is the case of Guess.com. In February of 2000, a visitor to the website was able to extract credit card information in clear text. In June 2003, the company settled charges with the FTC alleging that the company failed to take reasonable measures to protect customer data. In fact, the company failed to protect against the common threat posed by a SQL injection attack. This vulnerability was discovered by a visitor to the site who reported it to the FTC. In February 2002, PetCo, a popular retailer of pet supplies also lost data as a result of a SQL injection attack. Other breaches were caused by Cross Site Scripting (CSS) and Buffer Overflow attacks. In order to address these vulnerabilities, Visa USA began developing a set of guidelines to be used in the development of payment applications. The guidelines, the Payment Application Best Practices, are available online at the Visa USA website.

The Payment Application Best Practices (PABP) is a voluntary program for software vendors providing applications specifically for use in the processing of credit card transactions, as well as for companies creating in-house payment applications. It consists of 13 requirements that are believed to assist in securing the application against disclosing credit card information to

unauthorized individuals. Upon the successful completion of an assessment against the standard, Visa USA lists the companies and solution on their website. There are currently twenty-five companies listed on the website as having been successfully validated against the standard. While the PABP itself is voluntary, the PCI requires those that are governed by it to use only those applications, service providers, and vendors that enable compliance with the PCI and PABP validation can illustrate that.

Though compliance with the PABP is not mandatory it is strongly suggested that companies undergo an assessment against the standard. In fact, many processors are requiring PABP assessments, despite the fact that the card associations have not yet mandated them. As mentioned previously, merchants and service providers are required to ensure that their vendors can uphold the same standard of security as required by the Payment Services Industry. For those vendors whose business is providing payment software to merchants, adherence to the PABP demonstrates a commitment to security. That dedication to securing customer data can be leveraged as a competitive advantage in the industry. As more and more merchants seek to ensure their compliance with the PCI, they will be seeking out software vendors that are highlighted on the PABP-compliant list.

The other group to whom the PABP apply are those companies that develop their own, custom applications for accepting and processing credit card payments. These companies have a twofold reason to comply. First, complying with the PABP enables compliance with the PCI requirements. Requirement 6 of the PCI requires that companies “Develop and maintain secure systems and applications.” It further requires that any custom application be developed in accordance with industry

best practices and include information security in all stages of the development life-cycle. By assessing the custom application against the PABP, companies can demonstrate to the card associations and the industry at large that the company takes security seriously and that the PCI and PABP are critical considerations in the day-to-day business of the company.

The second, and perhaps more compelling reason, to comply is that it may demonstrate due diligence in the event that a breach does occur. With the best will in the world, there is no way to completely ensure that no breach will occur. Despite all precautions it is still possible that a zero day exploit or some other emergent attack may occur that has not been foreseen. In this event, it may become extremely important for the company to demonstrate that it has taken every reasonable effort to protect sensitive data from being disclosed. Having had the application assessed against the industry recommended best practices may serve as ample illustration of the company's attempts to counter the most common methods of attack.

Another reason that may compel companies to undergo an assessment, despite the voluntary nature of the program, is the increasing likelihood that the Best Practice will soon become a standard. As mentioned previously, retailers have become increasingly likely to be victimized by a data compromise. These attacks are coming more frequently through the payment application.

Compliance comparisons

Compliance Versus Validation

A common point of confusion with both the PCI and the PABP is the distinction between compliance and validation. Many believe that, since validation is not required than compliance is also voluntary. This confusion can lead to a variety of troubles, including fines and penalties. For that reason, it is necessary to reiterate that all companies, even Level 4 merchants, must comply with the PCI requirements.

Compliance, as will be discussed later, means that the company operates in accordance with the requirements. Validation is the process through which a company's or organization's compliance with an existing standard is verified. In the instance of the PCI, the method of validation may vary depending upon the size or level of the organization in question.

Though validation of compliance is not required for every company in the industry it may still be an important project to undertake. As previously discussed, the validation may serve as a competitive advantage. As the public becomes more and more aware of information security, successful security evaluations will likely have a greater impact on consumer confidence. Similarly, companies are becoming much more selective in choosing partners. There is a need to ensure that the prospective partner values data security to the same degree. An additional benefit of validating compliance even if it is not required is "safe harbor." If a company is found to be compliant at the time of the compromise, the card associations may refrain from imposing the fines generally associated with breaches.

The regulating agencies are another important audience to whom dedication to security should be demonstrated. As previously discussed, breaches can occur despite the

STORING CREDIT CARD DATA

most robust of information security programs. In the aftermath of a breach, it is likely that both the card associations and the government are going to request information regarding the information security practices of the company. The ability to produce documentation illustrating that the company was following industry best practice in the protection of data may be invaluable in mitigating fines and penalties associated with data security incidents. Many companies may object to validating compliance unless it is required. It may be viewed as an unnecessary expense. A more productive way to view validation, however, is in light of the fines that may be avoided.

Compliance Versus Security

In today's hyper-regulatory environment, the buzzword of the day is "compliance." Compliance projects demand significant portions of the information technology budget. Businesses are faced with a barrage of security requirements that must be met; from industry standards enforced by the major card associations, to state and federal regulations. Compliance projects are often difficult, time-consuming and, depending on the depth of remediation necessary, can be quite expensive. This being the case, the focus on compliance is understandable, some might even say it is commendable. The issue that arises from this singular focus on compliance, however, is that many companies are led to believe that "compliant" means "secure."

In order to understand fully the difference between the two, it is necessary to visit the definitions of the words. Stripped even of its regulatory context, compliance means "meeting or adhering to an existing goal or objective." This is a relatively static target. The foundation of compliance is a particular standard, such as the PCI, or objective, as

with a company policy. The policy or standard changes fairly infrequently.

This notion is significantly different than security, which has been defined as "a measure taken to guard against a threat or vulnerability." The goal of security is to mitigate the risk to the organization. As threats vary daily depending on the business environment in which the organization operates, it is necessarily a very fluid process.

Using these two definitions, it is clear that it is possible for an organization to be compliant, but not necessarily secure. The two concepts are not inherently inclusive of one another, and while it is not the objective of any compliance framework, occasionally the concepts diverge. For example, if a company holds its financial information in only one segment of the company network, and has deployed file integrity monitoring, intrusion detection and similar protections around that segment, it may be considered compliant with a particular standard or rule. However, it is entirely possible that these controls would not provide sufficient security as misconfigurations or other aspects have not been evaluated in terms of the risk exposure. It is important to remember that information security pertains not just to the information, but to the information systems that process and store that information. If the network is breached and employees are unable to access the systems, then the information security posture of the company has been compromised.

Similarly, it is conceivable that an organization could be secure without necessarily being compliant. If a company encrypts all personally identifiable information, the data may be considered secure, assuming it addresses the risk posed to the data and proper key management. The encryption of personal information might lead one to Consider the company to be secure even without the

benefit of information security training for the entire staff, which is a required element of the Payment Card Information Data Security Standards. In this instance, a company that operates in a secure manner would likely be grossly non-compliant with the PCI.

One way to illustrate this is to compare it to driving a vehicle. When a person owns a car, most states require that they have a safety inspection to ensure that it is not dangerous to operate on the roads. It takes into account the thickness of brake pads, the wear of the tires, the visibility of the window tint, the functionality of the tail and headlights, and similar safety aspects of the car. Upon passing the inspection, the vehicle owner knows that the car meets the specific safety standards set forth by the state. In other words, the car is compliant with state regulations for safety. However, the safety inspection does not evaluate whether the lug nuts are sufficiently tightened or if the fuel system is leaking. These are the traits that if applied correctly would make the vehicle safe, or in the vernacular of this paper, secure. Similarly, it is possible that the car could be perfectly safe, the lug nuts tightened and the fuel system properly functioning, yet not pass the safety inspection due to an excessively dark tint on the windows. In that case, the car would be secure, but not compliant with the safety regulations mandated by the state.

Today's businesses require a proper melding of the concepts of "security" and "compliance." The breadth and variation of the companies and organizations that are obligated by the laws and standards pertaining to information security preclude specific prescriptions. The standards and laws are purposefully broad so as to provide guidance on the issues without detailing the specific manner in which the objective is to be met. To do so would be unnecessarily, and in some cases unfairly, restrictive. It is therefore left to the organization to determine how to balance the

demands of regulatory compliance with the need for a comprehensive information security program. In this era of regulation and litigation it is likely prudent to err on the side of caution, implementing controls that are identified as necessary by a risk analysis, as opposed to simply meeting the minimum requirements of compliance.

Conclusion

The Payment Services Industry has been the focus of much discussion and debate over the past year. The frequency and magnitude of breaches has raised the awareness of the need for information security, above and beyond simply being compliant. Information security in the Payment Services Industry will only become an ever more prominent concern. The well publicized security incidents and increased congressional scrutiny in 2005 is likely to engender greater security awareness on all fronts. Both consumers and business will place more emphasis on the protection of cardholder data when selecting partners and vendors. Many in the industry are beginning to use a dedication to information security as a competitive advantage. This makes the implementation and maintenance of a comprehensive information security program critical, not only to compliance with the PCI, but to continued success as well. Though information security has not traditionally been considered crucial to business successes, in today's environment it is becoming increasingly clear that good information security is good business.

About the author

Dr. Heather Mark, Ph.D., CISSP specializes in regulatory compliance, privacy, and data security issues. She received her doctorate in Public Administration and Public Policy from Auburn University and is a Certified Information System Security Professional who frequently consults with companies within the payment services industry. Dr. Mark also writes a monthly article for Transaction World magazine on the topic of information security in the payments space.



1491 Center Crossing Road
Las Vegas, NV 89144-7047
Office: (702) 597-2480

1453 South Dixie Drive, Suite 250
St. George, UT 84770-5845
Office: (435) 628-5454

Fax: (702) 597-2499
Sales: (800) 265-5795

<http://www.shift4.com>