



Shift4[®]

Secure Payment Processing

Payment Security Solutions

The Gateway to Privacy and Confidentiality

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

May 2007

Executive summary

The proliferation of valuable data resulting from an increasingly interconnected world has made the protection of sensitive data critical to the success and viability of business. In fact, the protection afforded to data has become so central to the conduct of business that the rhetoric of privacy and security have even become commonplace in the private sector. Understanding the relationship between privacy and security can allow companies to achieve a more robust information program that addresses both issues. This paper will offer a brief insight into the current data security and privacy environment, followed by a brief explanation of the relationships between the two concepts. A brief gap analysis of security mandates and true security and privacy postures will be offered. Lastly, the paper will include a discussion of Shift4's philosophy on privacy and the ways in which Shift4's 4Go service can help a company establish a well rounded privacy program.

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 has become the currency of today's business. More than ever businesses rely on the exchange of information in business to business and business to consumer transactions. Shopping, paying bills, developing, and supporting business relationships all rely upon the exchange of information. In many cases, this information is sensitive or requires protection under various laws or regulations. The growth of information exchange has increased the risk that data may be accessed and used in a manner that is not consistent with the purpose for which it was first exchanged. Unauthorized access to this data may result from something as benign as third-party marketing efforts or as malignant as intentional data theft for the purpose of perpetrating financial crimes.

In the payment services industry, the increased focus on the use and protection of merchant data has had a profound impact. The advent of the Payment Card Industry Data Security Standard (PCI-DSS) and the Payment Application Best Practices (PABP) are tangible examples of the movement towards increased consumer protection. Few would argue anymore that the protection of data was not a valid a business function. The challenge that many businesses face today is bridging the gap between data security and data privacy.

Intersection of privacy and security

In the current business environment, it is common to hear the terms "data security" and "data privacy" used interchangeably. Such confusion is understandable given the media's preoccupation with data breaches and now the more than three dozen state laws requiring notification to individuals that may have been affected by those breaches. The result of this increased attention is an onslaught of vendors that have entered the fray promising to help ensure the security and privacy of sensitive consumer data. Often, the same vendors promising to help companies secure the data, and subsequently their customers' privacy, have little understanding of the differences between the two concepts.

It is not uncommon to hear the term data privacy used when in fact what is intended is data security. Understanding the two concepts is integral to the creation of a robust data protection program which includes the issues of security and privacy. Security, for instance, has been defined as "a measure taken to guard against a threat or vulnerability." The goal of security is to mitigate some risk to the organization. Further, these measures are employed to ensure the Confidentiality, Integrity, and Availability (CIA) of the data in question but do not ensure the proper use of sensitive information

The discussion of information security has been fairly common since the 1990s. Regardless, the adoption of standard information security practices has been slow to develop. The discussion of privacy as a business practice on par with information security has only come to pass within the past few years. Even now understanding of privacy as it differs from security can be hard to establish. Privacy has been defined by the International Association of Privacy Professionals (IAPP) as:

"...the appropriate use of personal information under

the circumstances...Also the right of the individual to control the collection, use, and disclosure of personal information.”

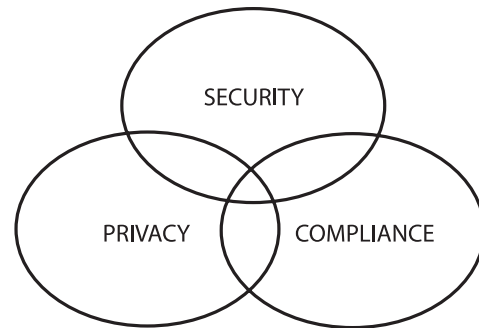
In essence, privacy is the assurance that the data collected from consumers will be used only for the purposes that the consumer approves. For example, selling customer lists to a third party without the consent of the individuals is a violation of privacy best practices.

The differences between data security and data privacy can be distilled to the following main points:

1. Security ensures that data is protected as it is stored and transmitted while privacy ensures that the data is used as it is intended by the consumer.
2. It is possible to have strong security practices without a clear privacy program, but one cannot have a comprehensive privacy program in the absence of strong security practices.

Adding to the confusion is a growing pre-occupation with compliance resulting from the litany of laws and regulations with which many companies must now adhere. Many organizations operate under the illusion that to be in compliance with a given standard or regulation is to be secure. In fact, the concepts of security, privacy and compliance are symbiotic, but not necessarily synonymous. It is possible that the three concepts, while symbiotic may diverge in certain environments. The relationship of these three practices can best be described as a Venn diagram.

In order to provide comprehensive protection and ensure that data is appropriately protected, a company should have an holistic approach to addressing data security and data privacy. By this, it is suggested that companies



consider security and privacy in conjunction as opposed to addressing the issues as separate projects.

While considering the collection and storage of data, one must also consider who can access that data and why. Additionally, companies must be aware of how that data is used and how it is shared. For example, once data is collected, is it then shared with a third-party provider to conduct marketing activities? Does that third-party provider have security and privacy practices that are the equivalent of your own? Given the regulatory and litigious environment in which businesses operate today, this type of information is crucial to mitigating the risk of a breach and to mitigating brand damage should a breach occur.

The ability to prove due diligence is paramount in defending against the myriad of compliance obligations companies are facing. Ensuring data is adequately protected guards your business from possible legal liability and civil penalties as well as the brand damage that invariably arises from publicized data breaches. The Internet is littered with news articles of good companies that have been ravaged by a single data breach resulting from a seemingly minor misstep in their information security and privacy practices. While some breaches are certainly more severe than others, unfortunately, in the eyes of the consumer and the media all data breaches are perceived as equally severe.

Industry regulation and legislative mandates

The payment services industry has been forward-thinking in its adoption of data security standards. The evolution of security in the industry has been remarkable although it is important to understand that addressing the security of information is only half of the equation. Companies must take measures to address the privacy of the data as well. While adhering to the PCI-DSS alone does not address privacy considerations, taken in concert with the state and federal mandates surrounding privacy, it does offer a considerable head start to the process.

Payment Card Industry Data Security Standard

Between 2000 and 2001, both Visa USA and MasterCard International introduced data security programs: the Cardholder Information Security Program (CISP) and the Site Data Protection (SDP) program, respectively. The two programs established a baseline of security measures required to be implemented by companies that were handling payment card account numbers and other Cardholder Data. Compliance with the programs was mandatory; however adoption of the programs in the industry was quite slow. Both American Express and Discover later 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 2003 data breach of Data Processing Incorporated (DPI), 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 brands began to collaborate on the creation of single, all-encompassing data security standard for the industry. In January 2005, the card brands introduced the Payment Card Industry Data

Security Standard, also called the PCI-DSS.

The PCI-DSS 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.

In 2002, Shift4 embraced the still nascent CISP standard and opted to undergo validation against this still voluntary program as a demonstration of their dedication to protecting cardholder data. As one of the first companies to be validated as “Fully Compliant” with the CISP, the precursor to the PCI-DSS, Shift4 made a definitive statement to the industry about their dedication to data security and protection of their merchant’s data. To this day, Shift4 maintains a close relationship with the card brands and other stakeholders in the industry to provide support and input into the various data security standards.

Shift4 hosted a Security Summit in the fall of 2005 and is currently a Participating Organization in the Payment Card Industry Security Standards Council. While these standards have introduced a new level of security to the industry, Shift4 has continuously encouraged the card brands to consider new rules that are even more comprehensive with respect to the security of cardholder data. In fact, Shift4 has taken steps to ensure that their

Compliance Difficulties

own operations and facilities exceed the security required by existing regulations and standards to ensure the safety of the data in their care. As an example of Shift4's continuing dedication to security Shift4 maintains a program that includes conducting comprehensive background checks, including employment history, criminal checks, financial and drug histories, on each of their employees. In addition, Shift4 ensures that their employees are aware of, and armed against, attempts to compromise data by means of social engineering.

Payment Application Best Practices

With the data security programs established and increasingly adopted, it was anticipated that the instances of cardholder data breaches would decline. Unfortunately, the Payment Services Industry had fallen victim to a new trend: the inherent vulnerabilities of insecure applications as the means to obtaining credit card information. It has become clear that the Achilles heel of the data security within the payment's industry is the lack of application layer controls.

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. It consists of 13 functional requirements designed 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 company and solution on their website in much the same way as they list PCI-DSS compliant organizations.

Understanding that sound information security practices are critical to business success, Shift4 has built its network Infrastructure and developed its applications with the

objective of providing the highest levels of security to protect merchant data.

Shift4 is responsible for developing custom payment application drivers for some of the most popular Point of Sale (POS) systems in use today. These include enhanced interface drivers for the Micros 3700, 8700, and 9700 systems. In addition to complying with the PCI-DSS, Shift4 has volunteered and paid to have these custom applications tested against the Payment Application Best Practices (PABP) to provide their merchants with the assurance that every aspect of the transaction that is handled by a Shift4 device or application is secure, and compliant. Each of the assessed applications was validated as fully-compliant with the PABP.

State and Federal Mandates

Many states, thirty-seven as of this writing, have taken action to require companies that have suffered a breach to notify those individuals whose data may have been compromised. Though these laws differ on a variety of issues, the underlying intent is the same – to ensure consumer privacy. While such laws may provide some benefit to consumers, it has proven cumbersome for many companies to comply with the various state notification laws. As an example, the definition of personal information, or non-public information, varies from state to state. California and Maine have essentially the same definition of personal data, except that Maine includes medical information in their definition.

For the most part, these laws indicate that a financial account number, stored in conjunction with customer name, address, or other identifiable information constitutes non-public information and a compromise of such data will trigger notification requirements.

STORING CREDIT CARD DATA

As one might imagine, the focus on security obscures the actual intent of the legislations – to ensure the privacy of customer data. These laws, however, seek to cure the issue of lax data privacy by addressing the symptom rather than the cause. Though many of the laws in question provide a safe harbor for data that is encrypted, that is frequently the only real data security technique they address. Nor do the state laws address the larger issues of data privacy – those surrounding acceptable use of the data and the ability of consumers to access and ensure the accuracy of the data.

The federal mandates, which are too numerous to discuss individually here, have made much greater strides towards the protection of consumer privacy. The galaxy of federal mandates surrounding data privacy is far more extensive than are the state laws. The Fair and Accurate Credit Transaction Act, Gramm-Leach-Bliley Act and similar legislation deal with the more broad issues of the acceptable use of data and the sharing of data among organizations. In addition to the growing pantheon of federal legislation dealing specifically the privacy of consumer data, the Federal Trade Commission has expanded its interpretation of the Federal Trade Commission Act (FTCA) §5A to include the protection of consumer privacy.

FTC §5A is the provision that allows the FTC to take specific actions to prohibit the use of unfair and deceptive trade practices. The FTC has determined that publishing a privacy or security policy, then failing to adhere to that policy, equates to a deceptive trade practice. Since 1998 the FTC has taken a wide interpretation of the clause, taking actions against companies that fail to provide adequate security as well as companies that share or sell data in a manner that is inconsistent with their published policies. The actions by the FTC are the only government action that

seems to address both issues of security and privacy. Their actions are largely derived from the Safeguard and Privacy rules of the GLBA, which are enforced by the FTC. It is often suggested that companies, regardless of their actual obligation to comply the FTC Safeguard Rule, use that document as a measuring stick for their own security programs. Should a breach occur and the FTC become involved, they will use that as a tool to assess to the comprehensiveness of the security measures taken by the company in question.

The Right of Private Action

A growing trend that should be of concern to all businesses storing sensitive customer data is the number of class action suits that derive from data breaches. Not only are affected individuals joining forces to hold companies accountable for lost data, but shareholders are becoming increasingly concerned with the effect of data breaches on stock prices. Some professional associations are lobbying Congress to hold merchants accountable financially for breaches of customer data. Add that to calls from some quarters to attach criminal liability to gross negligence resulting in exposure of data and the result has become an increasingly hostile environment surrounding the collection of storage and data in an era when businesses are ever more dependent upon the exchange of that information in order to do business.

To date, the success of class action suits surrounding the exposure of data has been questionable at best. While courts are willing to concede that such breaches have been inconvenient, the petitioners have been less than successful in proving negligence on the part of the company experiencing the breach or sufficient damages to the individuals or classes bringing suit. That is expected to change in the wake of the largest breach in history, that of

Tokenization

a large discount retailer. That breach has already been blamed for widespread fraud using the exposed data. One such scheme resulted in fraudulent activities amounting to over \$8 Million (USD) and the arrest of more than half a dozen individuals in Florida.

The result of the forgoing discussion is that, while many companies focus on compliance with PCI-DSS or other compliance mandates, their obligations are actually much more far-reaching. Rather than simply have the card brands and acquirers to face in the wake of a breach, companies face consequences from an expansive network of sources. It is imperative that companies understand not only their obligation to the mandates listed above, but to the principles of privacy as well.

The Privacy Gap

While the progress made by the Payments Industry is to be commended, the gap between the PCI-DSS and the legislative acts of the state and federal governments is vast. It should be noted that the PCI-DSS addresses only the security of the Primary Account Number (PAN) associated with payment cards and does not address any additional sensitive information. The data privacy laws that have been passed on both the state and federal levels are far more inclusive in terms of the definition of sensitive customer data. There is no discussion in the PCI standard of the privacy of related customer information, nor the security of any data other than the PAN. In that regard, the PCI-DSS is less expansive than the related legislation with which it is often grouped. On the other hand, however, the PCI-DSS goes much further than its counterparts in prescribing the methods through which the data should be protected. Regardless of the relative merits, though, adhering only to the PCI-DSS will not render a company compliant with the myriad of data privacy requirements

that exist today.

The PCI-DSS addresses only the data as it is stored and transmitted for its primary purpose – processing transactions. It does not address the use of the data, nor the rights of the merchant nor consumer with respect to that data. Most legislation in this arena makes provision for the customers’ ability to determine how, or if, their data can be used for secondary purposes – such as using the data for marketing purposes. The PCI-DSS does not make the distinction – if the PAN is stored it must be protected.

Though the PCI-DSS does have an extremely narrow focus, especially relative to the various state and federal mandates, it does begin the “level-setting” discussion with respect to comprehensive data protection and privacy methods. As companies begin the process of examining their data collection, storage and disposal practices as it relates to the PAN, it is natural to expand the scope slightly to include an examination of the treatment of all consumer data. It is important to note that compliance with the PCI-DSS will not ensure compliance with the various state and federal mandates regarding consumer privacy.

The gap between PCI-DSS compliance and true data privacy is becoming ever more important with the increasing numbers of class action suits that result from unauthorized disclosures of data. Not only will the FTC take action, but in many states laws provide for a private right of action for affected individuals. To date the outcome of these suits has largely been that, in the absence of proven damages, judges are finding in favor of the respondents. If, however, plaintiffs are able to prove negligence in conjunction with damages, as may be the case in recent retailer breaches, these suits are likely to be more successful. In order to mitigate the risk associated with data breaches, companies are advised to minimize the personal data that they store to that which is strictly necessary for the conduct of their business.

Shift4 philosophy on security and privacy

While compliance with the industry standards is exceedingly important to Shift4, the company's commitment to security was defined well before the industry took notice. Evidence of Shift4's dedication to security can be seen in the history of the company. Prior to focusing on providing Internet-based services, Shift4 was based on a Novell network. The company moved from this file-based network to a TCP/IP and serial network after identifying security issues in the file-based systems. In addition, the company recognized that the storage and transport of cardholder data offered the greatest risk both to Shift4 and its merchants. In order to solve this problem, and enable protection of data, Shift4 resolved to remove much of the burden of storage and transport of cardholder data from the merchant.

Security requires dedication, continual improvement and focused processes not simply the implementation of a specific technology or product. Understanding this Shift4 has ensured that security is integrated into every facet of their business. While Shift4 has consistently validated compliance against the CISP, then the PCI-DSS and PABP, the security measures enacted at the Shift4 data centers far exceed those requirements. At the data centers, Shift4 applies National Security Administration (NSA) C2 "Orange Book" security standards. These are the standards used by the most secure US government systems in order to ensure that these systems retain Top Secret clearance and are able to store, process, and transmit critical information vital to National Security. The Orange Book stipulates specific logical and physical access controls that must be maintained around sensitive data and is widely considered the most rigorous of the data security standards. While compliance with the PCI-DSS may appear challenging to some of Shift4's competitors, compliance with the

NSA standards is a great deal more challenging and further demonstrates the company's dedication to real security.

4Go establishes a foundation for security and privacy programs

A major foundation of information privacy, as well as a good rule of thumb for information security programs, is the simple adage, “If you don’t need it, don’t store it.” As simple as this may seem, it can be very difficult in practice. It is not unusual for companies to be unaware of the magnitude of sensitive information resident in their systems. Shift4’s 4Go technologies can help merchants end the problem of errant data storage before it begins.

Shift4’s dedication to minimizing the security burden of the merchant allows those companies to establish a strong foundation for security and privacy. In 2005, Shift4 created a new technology known as Tokenization. Tokenization was designed to provide even greater protection to Shift4’s customers by removing the storage of all cardholder data while enabling the customer to operate in a normal capacity. In keeping with Shift4’s philosophy of raising the overall security level in the industry, the company intentionally released Tokenization into the public domain.

Conceptually, the basics of Tokenization are straightforward. A transaction is swiped as usual at a Point of Sale terminal. Once transmitted to Shift4 for authorization, the information is converted into a representation of the data using a proprietary technology developed by Shift4. This data representation is known as a Token and is a globally unique, randomized representation of credit card data that is the same length as the original card number. After Shift4 receives the authorization response from the processor, the Token is then transmitted to the merchant while the sensitive authorization response, containing the card number, remains with Shift4 and is securely stored. This means that the merchant does not store the cardholder number in their systems. The Token was designed to be consistent with the size of a traditional card number to allow merchants to use the token as they

would traditional card numbers without the need to modify their existing applications or systems. For payment applications and merchants who utilize Shift4, only the Token is stored in the system.

The impact of a technology such as Tokenization can be enormous. As mentioned previously, the majority of state breach notification laws define personal data as some combination of identifying information, stored in proximity to a financial account number. If a merchant system is compromised and a Token disclosed, there is no way to link that Token to a particular individual. Following that logic, the unauthorized disclosure of the Token does not enable identity theft or financial fraud, which means that notification of the loss need not be made. It should be noted, however, that if the merchant is storing any unencrypted identifiable personal information (this may include social security number, driver’s license number, account numbers and similar information) that is compromised, then notification is still required.

In practice, Shift4’s 4Go Secure Swipe technology allows merchants to accept transactions while at the same time reducing the triple burdens of compliance, security, and privacy. As the card is swiped at the merchant location, the card data is encrypted using PKI technology prior to being received by the Payment Device. In other words, the merchant never holds any actual card data. At Shift4’s secure data center, the pre-authorization data is decrypted, formatted and sent to the processor for authorization. When the authorization message is returned to Shift4 from the processor, Shift4 then creates a Token and sends it to the merchant with the authorization message. Throughout the transaction, the merchant never holds sensitive authentication data. By processing the transaction in such a way, Shift4 removes much of the burden from the merchant. The merchant can focus again on their core

business – customer satisfaction, order fulfillment and similar activities. Shift4’s expertise provides a competitive advantage to their merchants.

The combination of 4Go Secure Swipe and Tokenization technology significantly mitigates the compliance and security burden of merchants. For example, PCI-DSS version 1.1 requires that merchants rotate their encryption keys on at least an annual basis.

The use of the 4Go Security Suite removes that burden from the merchant, as they never store any actual card data on their systems. An additional benefit of the use of such services is the continuity of security and privacy despite changing compliance mandates. Since the merchant is not storing cardholder data, they can be sure that they are protecting the privacy and security of that information. Compliance to industry or government mandates is a natural benefit to the use of Shift4’s 4Go technology.

Conclusion

It is important to understand that the 4Go Secure Swipe and Tokenization technologies may not completely remove the obligation of the merchant to protect any retained data. However, Shift4’s dedication to the protection of data can be used as a strong foundation for the building of a comprehensive data protection program. The evolution of data security standards, privacy practices, and legislative mandates is happening so quickly, that merchants often have a difficult time staying current with, and reacting to, the changes that are required to stay compliant. Shift4’s commitment to security and to their merchants, ensure that they are doing everything they can to ensure their products and services remain a powerful tool for compliance and for the protection of consumer privacy. Each merchant accepts a certain amount of risk when deciding to accept card payments and each consumer accepts a certain amount risk when using cards to pay for goods or services. Shift4 is actively re-defining the future of security and will continue to work with their merchants, solution vendors, and the payment industry to mitigate the risk to all parties.

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>