



Shift4[®]

Secure Payment Processing

Proactive Security Solutions for the Payment Industry

Tokenization and Best Practices in Payment Card Security

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

December 2006

Executive summary

In today's hyper-regulatory and litigious environment, the manner in which companies select partners and vendors has changed dramatically. Previously, companies made the selection based solely upon operating efficiencies, competitive differentiators and other strategic considerations. Increasingly, however, companies must also consider the manner in which potential partners and vendors protect sensitive data in order to protect their companies from risk associated with data exposure. As information security has become a major focus of consumers, governments and businesses alike, the care with which companies protect non-public personal information, such as credit card data, has become increasingly important. Shift4 has long been a leader in the payments industry, in particular with respect to the security of cardholder data. Dedication to security has always been a hallmark of Shift4's business philosophy and overall strategy. Evidence of this mission can be seen in the technological innovations of the company, as well as its partnerships. The following paper will illustrate the security leadership of Shift4 in the payments industry.

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.

About Shift4

Shift4, a leading developer of enterprise payment solutions, provides powerful, web-based applications that allow merchants to turn their customers' credit, check, debit or gift card transactions into dollars in the bank - quickly, accurately and securely. We work with our merchant customers, championing their cause and helping them to receive the lowest discount rates and fastest authorizations possible, regardless of the bank, processor or point-of-sale system they utilize.

Since 1994, Shift4 has provided real-time enterprise payment solutions to leading food & beverage, hospitality, retail, auto rental and e-commerce organizations worldwide, including Hilton Hotels, the PGA, Choice Hotels, Fox Racing, Build-A Bear Workshops, Louis Vuitton, Back Yard Burger and many other notable companies. Our forte is handling high volume accounts and enterprises with multiple entities, interfaces, locations, processors and merchant types all within the structure of a single system, giving merchants the ability to centralize control of all of their payment processes. This is accomplished through a powerful, innovative, unique, reliable and secure system that connects the world's most popular point-of-sale (POS) and property management (PMS) applications to the world's largest credit, debit and private label processors.

Shift4's vast experience within the payment services industry, coupled with its comprehensive understanding of the security issues facing the industry, allows the company to create simple, yet effective products that enable companies to conduct business efficiently, dependably and securely. Merchants may not have the resources, either financial or technological, to ensure the security necessary to survive in today's market. Shift4 can enable security while allowing merchants to focus on their core business.

Introduction

The Payment Services Industry has come under increasing scrutiny for what is perceived to be a lack of data security and incomplete protection of sensitive consumer data. A search through recent headlines reveals a litany of data breaches that have left retailers, payment processors, banks and card brands dealing with major public relations fallout. Correspondingly, the last two Congressional sessions have been littered with proposed legislation that would, if passed, regulate the manner in which data is stored, shared, and protected by companies. Additional Federal legislation being proposed may preempt the various state laws by creating a national notification law that would require businesses to inform customers when their personal data is, or may have been, compromised.

While difficult for some to understand, the increased security focus is not without merit. Statistics have shown that identity theft and financial fraud are among the fastest growing crimes in the world. Add to that the fact that the US has lagged behind other industrialized countries in defining data security legislation, and the focus on improving the security of personal data seems both inevitable and justifiable. While the public outcry and resulting legislative focus on increasing data security is relatively new in the US, Shift4 has long recognized the value and criticality of their customer's data and as a result has consistently been in the forefront of promoting greater data security and awareness. Additionally, Shift4 has been a leading advocate of increased Industry self-regulation and increased data protection requirements.

Data security and Shift4

Data compromises have been increasing at an alarming rate for the past several years. In 2003, the card brands identified less than 20 compromises while in 2005, more than 130 data compromises resulted in the exposure of over 50 million credit card account numbers. The growth in the number of compromises was accompanied by a corresponding shift in the compromise targets. Historically, payment processors and other data aggregators with large amounts of credit card data had been the preferred targets of data thieves. Supposition is that these targets provided a more lucrative payoff for the intruders, since they frequently housed millions, and sometimes tens of millions, of credit card account numbers. As these companies began to focus more on securing data, and likely because of the attention focused on their security by the card brands, the attackers increasingly shifted their attention to more traditional retail merchants and more specifically to hotels, restaurants, and other companies in the hospitality and travel and entertainment industries. While companies in the listed industries may not appear to be attractive data targets to the casual observer, they have become a favorite target of hackers. Although this trend is only recently being brought to light through data analysis, Shift4 has long recognized that retail merchants were at greater risk from hackers and other data thieves and as a result, have always ensured that their services were designed to counter these threats and protect the merchants' data.

While the credit card account number alone has limited value to a data thief, the data found on the magnetic stripe of the card is the focus of card thieves today. Obtaining only the second track of the magnetic stripe on the back of a credit card will enable the criminal to create counterfeit cards that can either be used as a traditional swipe card by the criminal or sold on the black market to other criminals. Since the magnetic stripe is not used to

Complete an Internet based (e-commerce) transaction, companies that specialize in online sales do not possess the valuable magnetic stripe data that thieves desire. In these types of transactions only the account number, name and card validation code (CVC2, CVV2), and in some cases the address (AVS), is required to authenticate the card. As such, criminals that compromise data from e-commerce merchants are limited in their ability to both perpetrate fraud and to sell the stolen data as there is insufficient information to counterfeit the cards. Since criminals using counterfeit cards are not restricted to perpetrating fraud through e-commerce sites, there is less risk of detection because the use of the card is not associated with a delivery address. In short, obtaining the magnetic stripe data allows for a greater return with less risk for the criminal. The end result is that brick and mortar retailers, as a general rule, are at greater risk of compromise than e-commerce merchants.

While retail merchants in general are more attractive to data thieves than e-commerce merchants, restaurants, hotels and other companies in the travel and entertainment segment are even more attractive targets. As the primary goal of data thieves today is to counterfeit cards to be resold, they are seeking cards with high credit limits and a low likelihood of fraud being reported by the user. Hotels and restaurants traditionally have a greater percentage of business travelers as customers. Additionally, hotels and restaurants tend to store more information in order to facilitate tips, late fees and similar associated charges. Consequently, the cards used by these customers are often corporate or business cards that typically have higher credit limits and the balances are often paid in full at the end of each month. In addition, many companies may be more willing than consumer users to accept fraud on their cards then report the compromise and risk potential damage to their company's brand. As such, these cards

provide a safer and much more attractive target for criminals.

While many gateways and other companies supporting merchant processing have taken a laissez-faire approach to information security and left their own customers (merchants) at the mercy of an increasingly sophisticated and dedicated group of data thieves, Shift4 has focused on a more proactive approach to protecting their customers. Founded when Internet commerce was still in its infancy, Shift4 recognized that the protection of their customers' data was critical to the success of their customers and took steps to ensure that security would be a central focus of their services. To support the security of their customers, Shift4 has ensured that the security of their merchants' critical data remains a primary business objective and a core competency of their own organization. Shift4 stands as a leader in payments industry for its dedication to securing cardholder data and in turn protecting their customers' business operations and reputation.

A profound example of Shift4's expertise and dedication to data security can be seen in the first solution the company developed to protect sensitive cardholder data in transport. This solution, which was developed solely by Shift4 and is still a core component of their offerings, is known as the Derived Unique Key Per Transaction with Moving Target Encryption (DuKPT w/ MTE) protocol. DuKPT w/MTE uses a peer reviewed security methodology that is unsurpassed by any employed on the Internet today. DuKPT w/ MTE secures transactions at an effective security level of 320bits, which is more than 200 times more secure than Secure Sockets Layer 3 (SSL3) using 128bit encryption. DuKPT w/ MTE is based upon proven IPSEC standard protocols like BlowFish and TripleDES. DuKPT (without Shift4's proprietary "MTE") is the same protocol that is used in the United States' Automated Teller

Machine (ATM) networks. The Moving Target Encryption (MTE) component of DuKPT w/ MTE changes the encryption method for every "leg" of a financial transaction's life cycle ensuring complete data content anonymity and confidentiality. Shift4 developed this technology before beginning work on any other application in order to ensure that this security protocol could be embedded in all of its products. As security is central to the core business of Shift4 all new products and services developed are molded around the DuKPT w/MTE technology.

While Shift4 was focused on ensuring that cardholder data was protected, the industry at large continued to view security as an unnecessary burden. Unfortunately, security incidents involving the exposure of cardholder data continued to increase at alarming rates in the late 1990's and early 2000. Naturally the card brands were growing concerned over the increasing incidents of fraud that resulted from cardholder data exposure, but there were other considerations as well. Inherent costs, such as consumer notification, card re-issuance, and fraud liability, while not directly impacting the card brands, were causing the card brands to take a more serious look at mandating the protection of cardholder data. Arguably a larger concern was of the growing potential for brand damage that occurs when credit card data is lost or stolen. As the card brands are responsible for maintaining and managing brands for the benefits of their member banks, damage to the brand results in damage to the entire payments industry. Finally, in response to the growing trend of data compromises, the card brands were feeling pressure to appear proactive to federal regulators who were increasingly threatening to push for newer and more rigorous legislation to regulate the payments industry. To address these concerns Visa and MasterCard began to independently develop their own data security programs.

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 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 associations 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 Standards, 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 customer’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. In fact, 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. While commending the card brands on their approach to data security, Shift4 feels that there are a number of key security issues that have not been adequately addressed in the regulations and standards currently affecting the industry. Among those key areas in which Shift4 believes the current standards are lacking are those surrounding physical security, social engineering and employee background checks. For these reasons, Shift4 has taken steps to ensure that their 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 route to unauthorized disclosure of 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 controls.

In 2006, MasterCard stated that one of the most common methods used to compromise cardholder data is the ubiquitous SQL injection attack. This attack may be familiar to those aware of the case of Guess.com which in February of 2000 was compromised through a SQL Injection attack and subsequently settled a claim by the Federal Trade Commission (FTC) which charged Guess.com with unfair trade practices. Because SQL Injection is such a common method of attack, the FTC charged that Guess.com was using unfair methods of competition by claiming in their privacy policy that they protected their customers' information while ignoring a well-know vulnerability. In February 2002, PetCo, a popular retailer of pet supplies also lost data as a result of a SQL injection attack. In addition to the SQL Injection attacks, compromises caused by Cross Site Scripting (CSS) and Buffer Overflow attacks begin increasing. In an effort to mitigate attacks such as SQL Injection that were occurring through the payment applications, Visa USA developed the Payment Application Best Practices (PABP) in 2004.

The 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 customer 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 and 8700 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 customers 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.

Shift4's continuing security leadership

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 commitment to security can be seen in the history of the company. Prior to focusing on providing Internet-based services, Shift4 was based on a Novel 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 customers. In order to solve this problem, and enable protection of customer data, Shift4 resolved to remove much of the burden of storage and transport of cardholder data from the merchant. The result was the introduction in 1999 of the payment services industry's first Application Service Provider (ASP) model supporting cardholder transaction processing. This ASP model, called DOLLARS ON THE NET, was the first step to removing the burden, and associated risk of merchants maintaining cardholder data and shifting the responsibility, cost, and risk to Shift4.

Security requires a dedication to 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 center far exceed those requirements by applying National Security Administration (NSA) C2 "Orange Book" security standards. These are the standards used by the most secure of US government systems in order to ensure that their 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 commitment to security.

The Shift4 data center also houses leased-line connectivity to all major processors and dial-up concentrators to minor processors to enable processing of transactions with unprecedented speed, accuracy, and security. All merchant data is securely maintained onsite at Shift4 using a family of products which are the finest and most secure financial transaction processing products in the industry. The data center also employs numerous security technologies specifically designed by Shift4 including "off Net" decryption and encryption of data for secure packet delivery, "off Net" database warehousing, and advanced firewall and connection logging technology. In addition, Shift4 uses systems that ensure TCP/IP delivery of Shift4 software based transactional packets only to ensure transaction integrity.

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 practices. The referenced Guess.com example provides evidence of such a scenario. 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. It is an unfortunate fact that losing several hundred or several

million records will likely have the same affect on the public's perception of your organization: Namely that your company does not protect the personal information of your customers. While data security is often difficult to understand and implement, it is vital to your organization's long term success. A study conducted in 2003 found that 50% of companies that experienced a data breach were out of business within 5 years. Put simply, sound information security practices not only enable good, sustainable business but are required to ensure the continued success of business.

Tokenization

Expanding upon the efforts initiated in 1999, Shift4 embarked on a new project designed to further protect customer's stored data. 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. 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 customer while the sensitive authorization response, containing the card number, remains with Shift4 and is securely stored. This means that the customer does not have to 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 Token spans the lifetime of the transaction, even allowing for searches into transaction archives, so it provides all of the same support for tips, tabs and incremental authorizations, and chargebacks as a stored card number would. Essentially, the Token is stored on the POS system, as the cardholder number would be in a traditional setup. When an incremental authorization is required on the card, the Token is sent to Shift4. Shift4

then easily translates that Token into the card data for transmission to the processor. The processor returns the authorization response and Shift4 converts the data into a new, unique Token, representing a new transaction. This new Token is then sent along with the approval code to the merchant. The authorization is completed and again no credit card data is stored on the merchant system.

In comparison with other Tokenization-type services offered by competing companies, Shift4's Tokenization offers a greater level of protection against compromise of cardholder data. Some providers allow their merchants to collect the card number along with the card identifier (roughly equivalent to Shift4's Token). Still others may require the merchant to manually register each card identifier. It is Shift4's belief that both of these practices entirely undermine the primary objective of Tokenization; namely to enable merchants to operate as normally as possible while not storing the sensitive data that is the target of data thieves.

Additionally, some service providers offering Tokenization-like services do not have adequate applications or application layer support to enable merchants to operate in a normal fashion while using a representation of data. This means that these service providers can not offer the necessary transaction reporting unless they allow the merchants to import the card numbers back into their point of sale systems and thereby defeating the purpose of their own solutions. Each of these competing methods undermines the purpose and goal of Tokenization: shifting the burden of security from the merchant to Shift4 and thereby reducing the likelihood of a data compromise or other serious event.

Partnering for better security

An example of the inherent insecurity of POS systems can be seen in the key management employed by many of the vendors. PCI-DSS requirement 3.4 mandates that merchants and service providers render stored cardholder data unreadable. In most cases this is accomplished through the use of encryption. In response to this requirement, many POS/PMS providers have incorporated encryption into their applications. Unfortunately, in many cases the key management in such a scenario is not sufficient to adequately protect the data or comply with the relevant standards.

It is not uncommon for a POS vendor to utilize cryptographic keys that are common among several merchants. That means that if one merchant is compromised, then all the merchants using that POS are also vulnerable and frequently compromised, as well. In another common scenario the merchant, who has little security experience, will be tasked by the POS vendor with the responsibility of managing the cryptographic keys for the application. Unfamiliarity with data security in general, and key management in particular, creates a glaring vulnerability at the merchant level and unfortunately results at times with merchants being found either non compliant or losing data. By partnering with select POS/PMS vendors, Shift4 removes the burden of key management from both the application vendor and the merchant.

One of the most difficult aspects of security to effectively manage is that of products and services provided by vendors or other third-parties. Shift4 recognizes that for most companies, security is not a core competency. In contrast, most have had security forced on them by regulation or by customer demand, whereas Shift4 focuses keenly on the protection of cardholder data and does consider security a core competency. In light of this focus, Shift4 works with select Point Of Sale (POS) and

PMS vendors to move the burden of securing data from those companies and onto Shift4. This allows the POS/PMS vendors to focus on their strengths while allowing Shift4 to shoulder the responsibility for protecting the merchant's data. Shift4's security integration with POS and PMS vendors is unique within the industry and protects the merchant from the vulnerabilities inherent in POS/PMS systems.

In addition to removing the burden of data storage from the merchant and POS/PMS vendors, Shift4 also eases the burden of compliance for merchants. By assuming the responsibility for storage of their merchants' sensitive cardholder data, Shift4 reduces the amount of data held at the merchant level. This allows the merchant to simply validate that no data is stored on site. If no data is stored, then the merchant has a significantly reduced PCI-DSS compliance burden.

Keep it simple

While information security may seem a complex process, it is often the less complex solutions that offer the best protections and greatest risk mitigation. In addition to an elegant simplicity, there must also be a complete understanding of security principles and the specific needs of the market. These three concepts, simple solutions, comprehensive security, and an understanding of the market are incompatible in many cases or not well understood in others. Some companies may chose to market their products as a complete security solution, yet have little understanding of the unique challenges faced by merchants in a particular market. Without such an understanding, merchants implementing such a solution may unknowingly be exposing themselves to greater risks. Merchants must be wary of such incomplete solutions, as they may introduce more problems than they solve. Similarly, other companies attempt to project an image of security expertise by creating complex solutions that purport to offer comprehensive security. The challenge in this scenario, and in information security in general, is that layers of complexity may obscure serious vulnerabilities in the product.

Continuing research and development

Security is something that no company will ever be able to completely guarantee as data security is very much an “arms race” that is constantly evolving and changing as threats are realized and vulnerabilities are exposed. As companies become increasingly savvy in the protection of their data, criminals are becoming more sophisticated in their efforts to identify and exploit vulnerabilities. Unlike many companies, though, Shift4 recognizes that security is an ongoing process, not a project or a single technology. Businesses must constantly evaluate their security posture and make adjustments to mitigate newly identified threats. Shift4 constantly works to evaluate new threats and take action to minimize their impact.

Shift4’s Tokenization solution has captured the attention of the card brands. Recently, Shift4 was invited as one of only two companies to participate in a MasterCard pilot program designed to evaluate the Tokenization solution and other security advancements in supporting the PCI-DSS.

Summary

Increasingly, companies are attacked using sophisticated technological methods and easily exploited vulnerabilities. Keeping abreast of the new exploits and attack methods makes the protection of sensitive data a challenging proposition for even the most security-minded of companies. Merchants are being targeted more frequently than ever before and with greater success for the criminal. In addition to the public fallout and brand damage that inevitably occurs as a result of a data compromise, current state and federal legislation exposes merchants to significant financial and legal liability should they be unfortunate enough to experience a data compromise. Those without the internal expertise to guard against the onslaught of data thieves are gambling with their company's assets. Shift4 has developed their business and their solutions specifically to help merchants handle the complex information security challenges inherent in the payment services space. Put simply, Shift4's suite of products can help mitigate the risk of accepting credit card payments.

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>