Outsourcing Payment Security
How outsourcing security technology is changing the face of ePayment acceptance practices
Table of Contents

The Issue: Payments/Card Data Security 3

What’s a Merchant to Do? Protecting Payment Data and Compliance 4

Beyond PCI with Tokenization – Next Generation Security 5

Deploying Tokenization via a SaaS Model 6

Homegrown or Vendor-Provided? 7

An Example of SaaS and Tokenization at Work 8

An Ideal Partner 9

Conclusion 9

About Paymetric 10
The Issue: Payments/Card Data Security

In recent years, new security applications and legislation have been put in place to protect sensitive card data. And for good reason. For corporations, the processes and requirements have proved difficult at best, crippling at worst. Merchants have struggled for years with cost-prohibitive payment integration systems, licensing fees and backbreaking requirements for payment processing.

Today, any merchant who accepts credit card payments is required to be compliant with Payment Card Industry Data Security Standards (PCI DSS). The best answer for merchants is to fully outsource payment-processing security, an option very few have chosen.

Even with the stringent requirements, security remains a major concern. If payment data is compromised, the financial and legal implications are enormous. Merchants risk regulatory repercussions, damage to reputation and financial penalties.

Additionally, according to a Deloitte survey, most C-suite executives would like to place a higher focus on risk and compliance moving forward. But breaches are still making headlines in the news. Research shows that a data breach costs an average of $5.4 million per company. With the total cost of a data breach at $136 per record in 2013, the financial impact to corporate America can be tremendous.

The Root of the Problem: An Inside Job?

So who is to blame for this breach in security? Of course, our first instinct would be to blame hackers, but the reality is not all data breaches are caused by outside sources. According to Forrester’s research, insiders are the top source of breaches in the last 12 months, with 36 percent of breaches stemming from inadvertent misuse of data by employees.

Companies are simply not doing enough to keep cardholder data secure. A high level of sophistication isn’t necessarily required for a cybercriminal to wreak havoc. Sometimes, all it takes is vulnerability, which often leads to data theft.

There are typically three areas of data vulnerability:

**IN TRANSIT:** data is moving from one device, application or system to another.

**AT REST:** data must be stored somewhere for later use.

**IN USE:** using data in a payment transaction is obvious, but card-holder data is also used for purposes other than a transaction (i.e., marketing using the data to support marketing programs, such as loyalty rewards).

One of the leading factors in data theft, and one of the top reasons a business is likely to fail a PCI DSS compliance audit, is the lack of protection of stored data – at rest or in use. The result is a rising cost of prevention and ever tightening PCI DSS compliance rules.

---

1 Deloitte Exploring Strategic Risk Survey 2013
2 Electronic Transactions Association (ETA)
3 Ponemon Institute 2013 Cost of a Data Breach: Global Analysis
4 Forrester Understand the State of Data Security and Privacy Report
What’s a Merchant to Do?
Protecting Payment Data and Compliance

In response to the ever-increasing worry and the growing costs associated with card security and electronic payments, the industry has been flooded with solution providers claiming the often-heightened protection for a merchant’s data. It’s clear that, in general, merchants don’t want the liability of having cardholder data throughout their enterprise.

Merchants are looking for solutions that will help them reduce or eliminate as many systems as possible from PCI scope. For each system moved out of PCI scope, merchants no longer need to deploy the 12 PCI mandated sections of security controls. In an effort to lessen the PCI workload, merchants often blindly invest in new solution offerings, in most cases out of fear, uncertainty and doubt. What companies don’t understand is that most of these solutions are not bulletproof and, therefore, not necessarily a good use of funds.

For merchants that handle, process or store cardholder data, the task of becoming compliant will become much more difficult as additional standards are instituted. Compliance will also become more expensive, with hidden fees built into the cost of the applications, ATMs, kiosks and mobile payment devices. The smart move in such a scenario is to minimize the amount of card data stored or flowing through the enterprise. But companies must be careful in what solution they choose to implement.

The strategic aspects of PCI require that merchants embrace technologies and procedures that enable the ongoing, operational management of data security and compliance. This means going beyond PCI to protect data in unconventional ways. The slow evolution of PCI standards gives technically advanced companies a window of opportunity to seek out technologies and techniques which will differentiate them in the marketplace, all the while allowing them to use the security of customer data as a marketing tool.

Tokenization, the next generation of card security, is the perfect example of “beyond PCI” technology. It can completely change how an organization manages confidential data across its various sales channels, divisions and applications.
Beyond PCI with Tokenization: Next Generation Security

With traditional encryption, when a database or application needs to store sensitive data, those values are encrypted and the ciphertext is returned to the original location. But there are three common challenges with basic encryption: cost, key management and application integration. For those organizations that have payment data in multiple, disparate systems, these challenges grow exponentially more difficult. Tokenization helps solve these issues.

Many people view the core definition of tokenization as the substitution of a credit card number for a meaningless replacement value that has no intrinsic value to criminals on the black market. But what is tokenization, really? A token can be thought of as a reference or pointer to a credit card number, without actually having to handle the credit card number. The bottom line is that tokenization is an evolution of the better known, but lesser qualified, traditional encryption. With tokenization, sensitive data is completely removed from enterprise systems. And, as an added bonus, the technology is complimentary to ERP systems.

Drilling deeper, tokenization affords companies that opportunity to eliminate the storage of sensitive information. This technology intercepts cardholder data entered into an enterprise payment acceptance system like a web store, CRM, ERP or POS, and replaces it with a surrogate number known as a token – a unique ID created to replace the actual data associated with a specific card number. This makes tokenization security best in class regarding data security. More than 25 percent of Gartner clients have already adopted payment card tokenization to reduce the scope of their PCI assessments, and three out of four clients calling about PCI inquire about tokenization.

By ensuring that business applications, systems and infrastructure are processing randomly generated numbers instead of regulated cardholder data, organizations can drastically reduce the controls, processes and procedures needed to comply with PCI DSS. This is particularly true if tokenization is provided to merchants as a service from a third party that maintains data management.

The task for merchants to find an electronic payment security solution that integrates into existing workflows while also:

- Protecting sensitive cardholder data
- Achieving and maintaining PCI DSS compliance
- Reducing the scope of compliance
- Conducting business as usual
- Deploying in a cost-effective manner

6 “Choosing a Tokenization Vendor for PCI Compliance,” Gartner – Avivah Litan
Deploying Tokenization via a Software as a Service (SaaS) Model

The SaaS model has flourished in recent years because of the many benefits it offers to merchants of all sizes and types. Here is what’s driving merchants to take advantage of SaaS solutions:

- Lower initial costs
- Painless upgrades
- Seamless integration

ERP systems have streamlined business processes and reduced the number of labor hours, allowing for automated processes in accounting, order entry, inventory management and human resources. And to further lower operating costs, manufacturers have increasingly outsourced some ERP services to third-party technology providers. Investments in new technologies are more likely to be funded if they help to achieve PCI DSS compliance, increase revenue or reduce cost without abandoning existing investments.

From the world’s largest corporations to small Internet stores, compliance with the PCI DSS is vital for all merchants who accept credit cards, online or offline, because nothing is more important than keeping your customer’s payment card data secure.

PCI DSS requirements have a tremendous impact on IT systems utilized by merchants who handle card processing because the process of compliance disrupts company operations and security guidelines. Thus, merchants that desire to dramatically reduce the hassle of PCI compliance are beginning to see the value of outsourcing payment processing to third parties.

Payment security outsourcing is a critical cost-saving component for any size organization. Small and mid-size organizations often find it a bit easier, however, to disentangle card data from their systems and procedures. Some of the merchants most interested in the combination of tokenization and payment outsourcing are eCommerce channel merchants and service providers. By eliminating the storage of sensitive cardholder data through a SaaS tokenization solution, merchants can realize a multitude of financial, operational and security advantages over traditional enterprise encryption solutions.

Merchants need to pay close attention to the collaborations between payment processors and technology solution providers to promote alternatives such as tokenization to fully eliminate stored cardholder data. Research indicates that CIOs and CISOs must develop a data storage plan that identifies sensitive data and its storage location, and establish adequate protection through access controls and encryption, tokenization or data masking while in transit, use and storage. A best-in-class practice is to not store cardholder data onsite.

With a tokenization solution outsourced via a SaaS model from a reputable vendor, cardholder data never resides in the merchant’s environment. The premise and theory behind encryption remains true – protect sensitive data with complex encryption algorithms wherever sensitive data is stored. Outsourced tokenization takes this principle to a new level: protect sensitive cardholder data by removing it from merchant systems entirely. Quite simply, merchants do not need to encrypt when they do not store. Let someone else shoulder the information and the burden.

Partnering with an enterprise payment integration and tokenization leader will also reduce the complexity of a company’s PCI audit. Because the merchant no longer stores cardholder data, they will comprehensively mitigate PCI Requirement 3, drastically reducing the time required to complete an audit. And the cost savings are felt throughout the process. A SaaS-based tokenization solution greatly reduces the cost of purchasing, installing and managing tokenization on-premise.

---

6 PCI Security Standards Council
7 “Simplify Operations and Compliance in the Cloud by Encrypting Sensitive Data,” Gartner Brian Lowans
Homegrown or Vendor-provided?

According to the PCI Knowledge Base, some large merchants with extensive and talented IT software development groups have considered developing a tokenization solution themselves. In most cases, the driving force was their homegrown experience with applications and databases that touched and stored credit and debit card data across multiple units. These companies found that, in actuality, adapting an existing tokenization solution to work with their homegrown applications would require exponentially more money than purchasing the product in the first place.

In a couple of cases, the companies did a performance analysis that concluded homegrown tokenization could have negative transaction processing implications. The PCI Knowledge Base’s research concluded that the homegrown approach to tokenization is still in the minority, as the talent and cost required is significant. Additionally, homegrown solutions tend to keep the sensitive data within the merchant’s four walls as opposed to partnering, which completely removes the merchant risk. The net take away is clear: leave it to the experts to deliver world-class solutions that reduce or eliminate risk.

Narrowly focused applications that are delivered via the cloud are great candidates for SaaS delivery, making integration back into the enterprise more manageable. Today, with pre-integrated SaaS solutions, businesses can quickly and affordably integrate payments into their ERP systems and at the same time completely remove cardholder data from their system. This makes PCI compliance a cinch and licensing fees a thing of the past.
An Example of SaaS and Tokenization at Work

A well-known, award-winning news and media corporation has a problem. With some newly enforced PCI DSS requirements in place, the encryption solution being used by the company for electronic payments (for subscribers, advertisers, etc.) is no longer sufficient in maintaining compliance. This means customers’ sensitive cardholder data is at risk and the company is now vulnerable to incurring fees and fines from the payment industry’s governing body.

To address this, the company implemented Paymetric’s XiPay® On-demand, a SaaS payment acceptance solution, and XiSecure® On-demand, a tokenization solution. Because the company would no longer be storing cardholder data, it would address the scope of PCI Requirement 3, making it no longer necessary to invest in a costly new encryption solution. While the decision to switch to a SaaS model was largely driven by compliance, the company realized it would experience the added benefits of reducing cost and risk when processing payments.

Those benefits translated into tangible assets. The company saved 143 percent on the cost per transaction when switching to Paymetric’s SaaS model. In addition, the new model reduced the time to complete the PCI annual audit by 80 percent, saving the company 20 percent on its PCI DSS compliance audit and $850,000 by eliminating the purchase of encryption technologies. Utilizing the SaaS model also reduced capital expenditures on enterprise payment acceptance solutions by 312 percent. And the company boosted its brand protection, since the sensitive information was removed from the internal servers, minimizing the risk of a breach.

In a Snapshot, Deploying Tokenization Via a SaaS Model Provides the Following Benefits:

1. No need to worry about card industry updates or upgrades (the credit card associations make at least two automatic updates per year)
2. No costly maintenance – it’s all taken care of offsite
3. No capital expenditures for licenses, hardware and servers (just a small monthly fee to process transactions)
4. Lower total cost of ownership (TCO) of payment acceptance
5. Quick startup, less time to deploy the solution vs. doing it in-house
6. Reduction of downtime costs – if something goes wrong, the solution provider remedies the solution immediately
7. Reduction of support costs
8. Scalable solution, particularly when opening new channels through call centers, web stores or new geographies
9. The opportunity to offer customers top-level card security by removing cardholder data from their systems entirely, utilizing tokenization technology
10. Protection of the company’s brand by reducing the risk of a data breach
An Ideal Partner

When choosing a partner, look for someone who is experienced in integrating within large corporate environments with different systems, not just a single application. Look for a solution provider that is proficient in SaaS delivery with the infrastructure in place to support an enterprise environment with maximum uptime.

There are material, technological, operational and most notably, financial considerations in selecting the right solution provider. One big mistake companies make is to discount the advantages of a specialized, secure, integrated payment solution provider brings to the table.

While there are some payment processors who offer their own tokenization solutions integrated with services, careful consideration should be given to a decision that ties a client to an environment that restricts their choices in the future. For example, by selecting a security solution from a payment processor or acquirer, what happens at the end of the contract term if the client wants to make a change to a different acquirer or processor?

Many questions need to be answered, including:

- What happens to my data?
- Who owns the data?
- How would I de-tokenize and move to a new provider?
- If I change processor, do I have to change my entire security layer?
- What specific experience does the acquirer or processor have with deploying solutions for ERP modules, web stores, call centers, integrated point of sale, kiosks, mobile payments and new emerging payment alternatives (i.e., what enterprise focus exists)?

In other words, serious consideration should be a given to select a solution provider that excels in sophisticated ERP environments and has the capability to leverage the significant investment a client has already made in their ERP foundation. Additionally, never underestimate that potential difficulty of integrating a tokenization solution within multiple environments. Finding a vendor with experience working within various systems will be an invaluable asset.

At Paymetric®, we bring an unrivaled level of experience and expertise. With solutions like Paymetric’s XiSecure, merchants have the opportunity to increase profits and sales while radically improving data security. With an eye towards the future, Paymetric’s XiIntercept™ solutions for XiSecure On-demand takes tokenization to the next level by ensuring that sensitive cardholder data never enters the enterprise payment acceptance system. And the process is entirely transparent to the customer.

The truth is, the burden of compliance and the associated expense, exposure and risk for merchants is only going to become more daunting. It is critical to choose a vendor that can lead the way by safely, securely and efficiently delivering viable solutions that enable clients to grow and manage their business.

Tokenization greatly reduces the risk of security breaches, operational expenses and negative public relations – all of which saves money and increases shareholder value.

Conclusion

With the continued changes occurring for card processors and merchants, tokenization is the only technology that will allow a CEO sleep at night. Implementing this technology via a SaaS solution provider makes more sense than ever before. For more information, visit www.paymetric.com.
About Paymetric

Paymetric, Inc. is the standard in secure, integrated payments. Our innovative payment acceptance solutions expedite and secure the order-to-cash process, improve ePayment acceptance rates, and reduce the scope and financial burden of PCI compliance. Leading global brands rely on Paymetric for the only fully integrated, processor-agnostic tokenization solution, supported by dedicated customer service. Paymetric is a nationally award-winning industry leader recognized for continual innovation, SAP partnership and world-class support since 1998. For more information, visit paymetric.com.