Protecting Cardholder Data Throughout Your Enterprise While Reducing the Costs of PCI Compliance

Breaches happen across all industries as thieves look for vulnerabilities. This is leading to the development of cost-effective and practical solutions to secure cardholder data at every point in the transaction lifecycle: in use, in transit, and at rest.

Elavon
Elevating Payments

Contents

Overview

Data Breach Costs Continue to Increase

Data security has become an enormous, global challenge. Cardholder data is particularly at risk — it's a favorite target of a growing legion of determined hackers and thieves because it is valuable and portable. With every advance in security, criminals seem to find more sophisticated and intrusive means of attacking merchant POS devices, back-office systems and network data centers. The attacks have graduated from local methods of pulling card receipts out of the trash or skimming a limited amount of cardholder data to using malware and sniffing technologies to capture millions of records to use globally.

While the number of compromised records dropped in 2010, there are more breaches than ever before. The financial impact of payment fraud is astounding. It has been estimated that total payment card fraud has reached $37 billion. The National Retail Federation in the U.S. estimates that merchants there have spent nearly $1 billion to remain compliant with Payment Card Industry (PCI) rules and regulations.

"The National Retail Federation in the U.S. estimates that merchants there have spent nearly $1 billion to remain compliant with Payment Card Industry (PCI) rules and regulations."

While no one is safe, the industries that have been by far the most severely impacted by costly payment data breaches are those related to hospitality, retail and financial services, which combined accounted for 60% of the breaches in 2010. Restaurants and hotels are a prime target because card transaction data typically sits on systems so that adjustments can be made (tips, extra charges, and so on) without the need for the actual card to be re-presented — making the information easier to capture. Retailers are next, responsible for 25% of the breaches, with some large brand-name companies recently making headlines. The average cost of a data breach has been estimated at $204 per customer record.

Unfortunately, breaches change consumer behaviors, with one study finding that 43% of consumers would avoid shopping at a merchant that had been breached, and another 31% of shoppers who would spend less at the merchant's stores. In addition to a loss of consumer confidence, businesses often experience damage to their brand or reputation, negative press and the disruption to operations. In some cases — for example, in the hospitality industry —a breach of a franchisee's property management system reflects poorly on the corporate parent of the flag, regardless of whether there was corporate involvement. Eliminating card data entirely can disrupt

business processes since card numbers provide unique customer information. Clearly, this combination of damage to reputation and business loss can be devastating — potentially threatening the ability of a merchant to remain in business.

PCI Compliance Guidelines

The payment industry has made significant strides in responding to security threats since the PCI Security Standards Council was formed by bringing together the efforts of the various card schemes — with the first set of PCI standards and practices released in 2004.

Any business that processes, stores or transmits cardholder data is required to comply with the PCI Data Security Standard (DSS). The PCI DSS is a set of constantly evolving requirements intended to help merchants and businesses that accept electronic payments proactively protect customer account data. The standards require maintaining a secure network, implementing internal controls and performing regular testing. These best practices have been revisited and enhanced multiple times over the past few years, with the latest version being PCI Payment Transaction Security (PTS) 3.0 — which added several new modules addressing open protocols, integration, and guidelines for the more secure reading and exchange of data.

It's important to note that PCI compliance alone does not protect against an attack. There are often too many potential points of failure. It's fair to say that organizations are only PCI compliant until they are breached; somewhere along the line your systems could become vulnerable to an attack.

"It's fair to say that organizations are only PCI compliant until they are breached; somewhere along the line your systems will become vulnerable to an attack."

So what can you do to overcome these challenges? By finding solutions that:

- Protect data throughout your enterprise
- Provide for business process continuity
- Mitigate the costs and complexities associated with PCI compliance

Maintaining PCI DSS compliance is a continuous practice that is complex, time consuming and expensive. Let's start with a brief overview of the current technology advances that are helping companies protect data, while easing some of the burdens associated with PCI compliance.

A Comprehensive Approach to Payment Security Solutions

Staying One Step Ahead

It should be no surprise that PCI compliance alone does not protect against malicious attacks by thieves. Each advance in payment system security seems to be countered by a new method or technique from hackers. The reality is that these threats are constantly changing and becoming more dangerous. This is underscored by the number of high-profile breaches that larger retailers, processors and acquirers have suffered recently. These businesses may all have had payment security solutions that were certified as PCI compliant, but they still had their systems compromised.

Payment data security is both figuratively and literally a moving target. To counter threats and achieve true peace of mind, you need security solutions that protect cardholder data at every step in the transaction lifecycle:

- In Use — While being used throughout an enterprise for post-authorization, card on file adjustments, analysis and reporting
- In Transit — From the earliest point of entry in the data stream and while traveling to and from a gateway or processor
- At Rest — While being stored in a batch or on a system

> "To counter threats and achieve true peace of mind, you need security solutions that protect cardholder data at every step in the transaction lifecycle... in Use, in Transit, at Rest."

Organizations can secure critical data by implementing advanced solutions that encrypt or mask cardholder data. It's important to note that not all solutions are the same. Look for end-to-end solutions that are secure, flexible and comprehensive.

EMV

EMV is a global standard for payment cards based on chip technology developed in 1994 by Europay International SA (acquired by MasterCard in 2002), MasterCard and Visa. EMV helps authenticate the cardholder and therefore reduces the fraud associated with purchases made with counterfeit cards at a physical point of sale.

EMV terminals read advanced algorithms contained on chip cards to authenticate that the card is not a counterfeit. The data is not encrypted or secured for processing the transactions. Cardholder data is more secured on a chip-embedded card that utilizes

dynamic authentication, rather than on a static mag-stripe card. Unlike a mag-stripe card that can be copied ("skimmed"), chip technology combats counterfeiting by assigning a dynamic value for each transaction.

The data is not encrypted or secured for processing the transactions. While EMV goes a long way to prevent counterfeit card use, it's important to note that EMV alone does not encrypt or secure card data for processing the transactions. You will want to implement EMV devices that also support point-to-point encryption and help de-scope the POS.

Point-to-Point Encryption (P2PE)

P2PE encrypts the card data at the earliest point of entry to protect it as it travels across various systems and processing networks. It uses key algorithms to make card data unreadable to anyone without access to a special key code. Look for a P2PE solution that protects data from the instant a card is swiped or keyed on a terminal featuring a hardware-based, tamper-resistant security module — and keeps it encrypted until the data has traveled to a centrally-located, secure data center (in transit) for decryption and processing.

Additionally, solutions that feature format-preserving encryption, which retains the original length and structure of card track data, minimize or eliminate any adverse impact on your POS systems or message formats. And if you need to connect with multiple processors, choose a provider that supports P2PE, which secures data at the point of capture through to a payment gateway.

Tokenization

Tokenization converts or replaces cardholder data with a unique token ID consisting of random strings of characters to be used for subsequent activity, while storing the original data and token algorithm in a centrally-located, secure data center. It eliminates the possibility of having real card data stolen because it no longer exists in your environment, while allowing you to use the token in place of the Primary Account Number (PAN) for necessary tasks.

"It eliminates the possibility of having real card data stolen because it no longer exists in your environment, while allowing you to use the token in place of the Primary Account Number (PAN) for necessary tasks."

Tokens that represent cardholder data reside on a merchant's POS/PMS (at rest), and are used to make adjustments, add new charges, make reservations, or perform other transactions (in use). If you will be making adjustments, you'll want tokens that are based on the card, not a transaction, so that the token can be used whenever that card number is presented again.

End-to-End Protection

The combination of EMV, P2PE and Tokenization will extend peace of mind to your financial, security and operational executives, allowing them to focus on initiatives that drive your business forward, knowing that card data cannot be compromised.

Look for a solutions provider that offers secure multi-point connectivity across your enterprise. When you have multiple providers and/or a third party gateway, there are more possible points of failure or PCI exposure to detail in your compliance reporting, which add complexities to your business.

Your provider should also host and maintain the decryption service and token vault. Otherwise, they must utilize 3rd party data centers or remote locations for decryption or tokenization, adding latency and more potential failure points in the authorization cycle.

Last, ensure that your provider is experienced and financially strong, with networks running on stable and redundant systems, managed and monitored by a knowledgeable, responsive IT team.

Business Process Continuity

Very importantly, you want to be able to encrypt data without requiring changes to your POS software and message formats. This way, you can protect data without impacting the way that you utilize customer card information – card-on-file transactions, shopping analytics, loyalty programs, operational requirements, and other processes. This allows your business to store the tokens indefinitely without the fear of compromising sensitive data – leaving you time to focus on projects that contribute to revenue or operational efficiencies.

> "You can protect data without impacting the way that you utilize customer card information– card-on-file transactions, shopping analytics, loyalty programs, operational requirements, and other processes."

Mitigating the Costs and Complexities of PCI Compliance

Top Priority: Get it Out!

With the increasing risks and costs associated with payment security, businesses from all industries are crying in unison — get it out! You want the cardholder data that subjects you to potential fraud out of your store or off your property — away from the enterprise.

When you remove actual cardholder data entirely from the payment stream, you can shift responsibility and risk to your provider by moving elements of the security process "upstream." Thereby, you can limit and reduce your scope of PCI compliance and also reduce expenses.

Improving Protection, Increasing Expenses

PCI compliance is not a one-time effort — it is a continuous process that requires ongoing attention and a commitment of resources to monitor and maintain systems. A key element of this is the PCI audit process, which was implemented to assist larger, Level 1 (process over 6,000,000 transactions per year) merchants in validating compliance with PCI DSS. Any part of your systems that are related to accepting, authorizing and settling payment data is "in scope" for compliance validation.

> "PCI compliance is not a one-time effort — it is a continuous process that requires ongoing attention and a commitment of resources to monitor and maintain systems."

Level 1 merchants must have an annual onsite review by a third party Qualified Security Assessor (QSA). All other merchants have the opportunity to complete a self-assessment, in some cases with additional requirements attached (such as a mandate to attend authorized PCI Security Standards Council training).

A Hefty $1 Million Price Tag

As you might imagine, the cost of maintaining PCI compliance can be quite high, averaging $1 million annually for many Level 1 merchants. This includes ongoing audit and system scanning costs to adhere to the requirements, plus increased costs to monitor and maintain systems. These expenses are expected to rise as the standards become increasingly sophisticated, and require more complex and costly support and annual assessments to maintain and verify.

The Upside to Advanced Security Solutions

In addition to protecting systems from a potential breach, implementing EMV, P2PE and tokenization solutions may reduce, eliminate or shift some of the responsibilities of PCI compliance from the merchant to a third-party gateway provider or acquirer. Removing actual cardholder data from the merchant's environment may allow the merchant to shorten or even avoid entirely part of the audit process, saving time, labor and money, even allowing for the redeployment of valuable resources.

Responsibility and fines shift whenever an element of the security process is moved further up in the transaction lifecycle — above the property or in the cloud — by utilizing hosted gateways, decryption appliances and token vaults. The ability to bypass the POS completely when transmitting data may significantly reduce or eliminate POS workstations from the PCI audit process.

"Removing actual cardholder data from the merchant's environment may allow the merchant to shorten or even avoid entirely part of the audit process."

Conclusion

Protecting Payment Data and Your Bottom Line

The process of securing cardholder data and maintaining PCI compliance seems to become more complex and costly each year. Yet with the growing threats to payment information, to effectively protect your cardholders and your company's reputation and enjoy true peace of mind, you need a sophisticated solution that protects data at every phase within the transaction lifecycle: in use, in transit and at rest.

Introducing SAFE-T Suite from Elavon

Elavon has built upon its leadership in the payment industry to design a portfolio of security solutions and services that can help companies secure cardholder data, ease the burden of complying with changing PCI compliance regulations and ensure business processes continuity. Our solution SAFE-T Suite stands for Secure and Flexible Tokenization & Encryption.

Businesses that rely on SAFE-T Suite for payment security can protect data at every stage of the transaction lifecycle: in use, in transit and at rest. Elavon's SAFE-T Suite is a portfolio of comprehensive payment security solutions that can be tailored to your precise requirements — to help mitigate risk and potentially shift much of the responsibility for data breaches to others, in addition to reducing the costs of PCI compliance on an annual basis.

> "Elavon's SAFE-T Suite is a portfolio of comprehensive payment security solutions that can be tailored to your precise requirements."

SAFE-T Suite helps companies modernize their security strategies and successfully combat evolving security threats:

- Remove actual card data from the payments stream
- Utilize EMV, P2PE and tokenization to protect data in Use, in Transit and at Rest
- Seamlessly integrate terminals that support EMV and P2PE with leading POS/PMS systems
- Ensure the continuity of existing business processes that require the use of card data
- Reduce the costs and complexities of PCI compliance

Elavon offers 20 years of global payment processing and gateway experience. Our knowledgeable team of experts can assist with solution design and implementation as well as deliver a wide variety of professional and managed services. And we are backed by the full strength and stability of U.S. Bank.

For decades, retailers, hospitality businesses and other enterprises have invested a great deal of time and money into ensuring that their physical stores or properties are as secure as possible against theft, fraud and other criminal activities. With a substantial percentage of the threats today shifting to information networks, Elavon can guide you in making wise investments in data protection, PCI compliance and reducing the total cost of card acceptance.

To learn more about payment security and SAFE-T from Elavon, contact your Elavon representative.