



Managing the Costs of Securing Cardholder Data

The costs and complexities related to protecting cardholder data and complying with PCI regulations have become burdensome for most organizations that accept card payments. This is leading to the development of practical solutions to secure cardholder data at every point in the transaction lifecycle: in use, in transit, and at rest.



Contents

3	Overview: Payment Security: A Complicated, Costly Challenge
4	Payment Security is a Process, Not a Product
5	A Secure, Flexible and Comprehensive Approach to Payment Security Solutions: Top Priority: Get it Out!
5	Trying to Stay a Step Ahead
6	End-to-end Encryption (E2EE)
6	Tokenization
6	Hosted Payment Gateways
7	Configuration Options
7	End-to-end Control
9	Mitigating the Costs and Complexities of PCI Compliance: Improving Protection, Increasing Expenses
9	\$1 Million Price Tag
10	The Upside to Advanced Security Solutions
11	ROI Analysis: Real-world Information That Demonstrates How the Right Solution Can Pay Dividends for You
13	Conclusion: Protecting Payment Data and Your Bottom Line
13	Introducing SAFE-T Suite From Elavon



Overview

Payment Security: A Complicated, Costly Challenge

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. With every advance in security, these criminals seem to find more sophisticated and intrusive means of attacking merchant POS devices and systems, as well as processor data centers. The attacks have graduated from 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.

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 industries that have been by far the most severely impacted by costly payment data breaches are those related to hospitality, food and entertainment, which combined accounted for 67% of the breaches in 2010. Restaurants and hotels are a prime target because card transaction data typically sits on their 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 18% of the breaches, with some large brand-name companies recently making headlines.

“It has been estimated that total payment card fraud has reached \$37 billion. U.S. merchants have spent nearly \$1 billion to remain [PCI] compliant.”

Data breaches can be costly for businesses in a variety of ways. From a financial standpoint, breached merchants face significant fees and fines from the card associations. But that's just the beginning. You must also pay for requirements such as notifying customers of the breach, investigating how the breach occurred, and often, covering large legal fees to defend your business against expensive class-action lawsuits. The average cost of a data breach has been estimated at \$214 per customer record.

But beyond these “hard” costs, there are many “soft” costs such as damage to your brand or reputation, negative press and the disruption to your operations as you try to work around the breach. In some cases — for example, in the hospitality industry — a breach of a franchisee's property management system would reflect poorly on the corporate parent of the flag, regardless of whether there was corporate involvement.

There can also be a negative impact on consumer behavior, 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. Clearly, this combination of costs and loss of business/damage to reputation can be devastating — potentially threatening the ability of a merchant to remain in business.

Payment Security is a Process, Not a Product

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.

So what can you do to overcome these challenges? Some merchants search for the best security product — one that can meet all of their requirements and help protect their systems from a data breach. Companies are seeking solutions that:

- Secure cardholder data against attacks
- Mitigate the costs and complexities associated with PCI compliance
- Lower the total cost of card acceptance.

But it's important to know that payment security is a process, not a product. No two industry verticals have precisely the same exposure or risk factors. And individual merchants within each vertical may have far different strengths and weaknesses, contributing to a vastly different set of requirements.

Consequently, it's necessary to employ a process-oriented approach to addressing security requirements for your organization. Representatives of all key departments — Finance, Security, IT, and Operations — should meet with solution providers and work together to consider a range of factors including your specific industry, the point-of-sale (POS) or property management system (PMS) you rely on, your specific card acceptance environment, how you use cardholder data post-authorization, and your appetite for risk tolerance. And as always, your organization most likely does not have an open checkbook. Therefore, costs and operational impacts need to be analyzed.

“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.”

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 Secure, Flexible and Comprehensive Approach to Payment Security Solutions

Top Priority: Get it Out!

With the increasing risks and costs associated with payment security, merchants 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.

What you need is a solution that protects data by either masking account numbers or, better yet, removing actual cardholder data entirely from the payment stream. In addition, this should reduce the costs and complexities related to the PCI compliance process.

Trying to Stay a Step Ahead

As was stated earlier, 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.

“It should be no surprise that PCI compliance alone does not protect against malicious attacks by thieves. Threats are constantly changing and becoming more dangerous.”

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** — At the earliest point of entry into the data stream
- **In Transit** — While being sent to or from a processor
- **At Rest** — While being stored in a batch or on a system for possible post-authorization uses, adjustments and reporting.

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.

End-to-end Encryption (E2EE)

E2EE uses key algorithms to make card data unreadable to anyone without access to a special key code. Look for an E2EE solution that protects data from the instant a card is swiped in a hardware-based, tamper-resistant security module to where card data is keyed into an application or for a card not present scenario (in use) — and keeps it encrypted until the data has traveled to a centrally-located, secure data center (in transit) for decryption and processing. Solutions that only encrypt at the software application layer of the POS could still be subject to malware or “man in the middle” attacks.

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 Point-to-Point Encryption (P2PE), which secures data at the point of capture through to a payment gateway (and beyond).

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. 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. 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. Finally, make sure that you can support a token-only request, so that you aren’t paying an authorization fee if you need a token for a non-financial transaction.

“Gateways provide secure multi-point connectivity across an enterprise, while protecting data in a centrally located secure data center.”

Look for flexible tokenization solutions that support single use, multi-use, recurring, and card-on-file use cases mapped to your business needs. Consider different token structures — numeric, alphanumeric or POS system-specific — based on your expected business uses. Make sure that the provider you choose can offer a variety of token use cases — your needs will vary even within your enterprise. For example, the spa in the hotel may require tokens for card data at rest in the profiles of customers, while the restaurant may only receive tokens upon authorization request.

Hosted Payment Gateways

Gateways provide secure multi-point connectivity across an enterprise, while protecting data in a centrally located secure data center. A merchant such as a hospitality customer can have transactions sent from multiple points of payment — the front desk, spa, retail shops, restaurants, poolside — to multiple processing endpoints, and still benefit from E2EE and tokenization.

In addition, gateways provide the flexibility to add or change processors as needed, without changing encryption and tokenization schemes — you are able to support a consistent method for E2EE and tokenization, regardless of acquiring endpoint.

Configuration Options

Every business has its own level of preparedness and vulnerabilities — as well as tolerance for the risk of losses — associated with payment security. It's important to quantify your level of risk for data breaches and fraud, identify any particular points of vulnerability, evaluate the appropriateness of your POS/PMS systems, and discuss your approach to PCI audits.

Choose a provider that offers a number of configuration options in deploying a payment transaction security solution, simplifying PCI compliance and potentially even extending the life of legacy POS systems — reducing your costs. Examples of flexible configuration options include:

- **POS Bypass** — The ultimate choice for getting cardholder information out of your POS. A solution that transmits encrypted cardholder data on an alternative secure network path — bypassing your POS entirely from card swipe to a hosted gateway and back — greatly reduces your POS workstations from within the scope of PCI compliance.
- **Gateway Terminal Solutions** — These allow standalone payment terminals to securely communicate directly to a hosted gateway, while providing visibility into consolidated transaction activity.
- **Peripheral Device Managers** — These software solutions facilitate the transmittal of payment data between POS terminals and payment devices, IP terminals, and a hosted gateway — simplifying POS integration.
- **Key Management** — Key rotation/management methodology built around the strength of the keys, including algorithms to make card data unreadable to anyone without access to a special key code.

“Choose a provider that offers a number of configuration options in deploying a payment transaction security solution, simplifying PCI compliance and potentially even extending the life of legacy POS systems.”

End-to-end Control

Finally, look for a solutions provider that is experienced and financially strong, with networks running on stable and redundant systems, managed and monitored by a knowledgeable, responsive IT team.

You can't expect to always do it all. Solution providers should offer solutions design and implementation services, as well as ongoing support. And for a true outsourced solution, inquire about a provider's ability to offer PCI audit analysis, where experts assist and advise you on your PCI compliance process and identify potential "de-scoping" opportunities to decrease the burden on your business.

Finally, make sure that you work with a provider that has tools to assess your Return on Investment (ROI), so that you can monetize solution costs, data breach risks and PCI compliance audit reduction opportunities. This can help you determine the most appropriate and cost-efficient solution to obtain the cardholder data protection your business requires.

We'll take a closer look at this at the end of this paper.



Mitigating the Costs and Complexities of PCI Compliance

Improving Protection, Increasing Expenses

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 issuers — with the first set of PCI standards and practices released in 2004.

Any merchant 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.

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.

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).

\$1 Million Price Tag

As you might imagine, the cost of maintaining PCI compliance can be quite high, averaging \$1 million annually for Level 1 merchants. This includes ongoing audit and system scanning costs to adhere to the requirements, plus increased costs to monitor

“PCI compliance is a continuous process that requires ongoing attention and a commitment of resources to monitor and maintain systems.”

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 E2EE and tokenization solutions may reduce, eliminate or shift some of the responsibilities of PCI compliance from the merchant to a third-party 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. With hardware-based E2EE, data is encrypted at the earliest point in the transaction lifecycle, and may never enter the POS/PMS system. And tokenization mitigates the PCI compliance requirements that address stored cardholder data, and access to data on a business need-to-know basis.

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.”



ROI Analysis

Real-world Information That Demonstrates How the Right Solution Can Pay Dividends for You

To repeat an assertion made earlier in this paper — the steps taken to implement a robust end-to-end security solution represent a process, not a product that is taken off the shelf. No two businesses are alike. Retailers, government agencies and universities have very different requirements from those of a large hotel or restaurant groups that may oversee a variety of flags or brands. And while it's nice to know the estimated savings from effectively protecting cardholder data while decreasing the expense and effort required for PCI compliance for the average business — you want proof, and you'd like to know specifically how much these measures could save for you in real-world situations. Elavon is pleased to introduce a proprietary and exclusive ROI model, which makes that information readily available to you.

Using Elavon's ROI model, your individually tailored analysis will begin with an examination of those elements of your business profile that can impact your costs for PCI compliance.

- How many stores/properties do you own?
- How many points of payment do you operate in each location?
- What is your current transaction volume, and what is the average growth rate in transaction volume?
- What is the state of your PCI compliance program? Are you compliant now?

Costs can then be calculated and scrutinized within the ROI model in each of several major areas:

- **Data Protection** — What are your actual costs for implementation, ongoing monitoring and transaction fees (if applicable)? And what kinds of protection do you need? A hospitality client will likely want both end-to-end encryption and tokenization, where a retailer may only need E2EE because they don't perform subsequent transaction adjustments.
- **PCI Costs and "De-scoping" Opportunities** — What are your current costs for the 12 steps of PCI compliance, as defined in the regulations? How much will you spend on annual PCI DSS audits, building and maintaining a secure network, protecting cardholder data, maintaining a vulnerability management program, maintaining an information security program, and so

“While it's nice to know the estimated savings... you want proof, and you'd like to know specifically how much these measures could save for you in real-world situations.”

on? And how much can you decrease those costs by moving the risk of data breaches off your premises through effective cardholder security measures?

- **Breach Impact Cost Savings** — Keep in mind that you are only PCI compliant until an actual breach occurs. Therefore, the model contains average costs per-record of dealing with a potential data breach: for detection/escalation, notification, ex-post response, and the impact in lost business or diminishing of your brand. With an average breach for a Level 1 or Level 2 (process 1,000,000 to 6,000,000 transactions per year) merchant today involving more than 33,000 records, it is easy to see how quickly the costs add up.

Finally, the model brings everything down to the bottom line — indicating what an effective data protection solution costs and what your potential savings could be by reducing PCI DSS audit fees, decreasing the other costs of PCI compliance and avoiding the substantial expense of a potential data breach. With these real-world figures tailored to your business, you will be able to make much more informed decisions regarding the payment security your business requires.

“With an average breach for a Level 1 or Level 2 merchant today involving more than 33,000 records, it is easy to see how quickly the costs add up.”



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 burdens of complying with changing PCI compliance regulations and lower the total cost of card acceptance. We have named this array of solutions SAFE-T Suite, which stand for Secure and Flexible Tokenization & Encryption.

Businesses that rely on the 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 secure, flexible and 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. Our exclusive ROI model can provide an accurate picture of the true costs you face and the potential cost savings and risk avoidance you can attain with the right payment security solutions in place.

“Elavon's SAFE-T Suite is a portfolio of secure, flexible and comprehensive payment security solutions that can be tailored to your precise requirements.”

Elavon offers 20 years of global payment processing and gateway experience. We can perform complete PCI DSS audits, handle solution design and implementation, and 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, or to request an ROI analysis, visit www.gateway.elavon.com, or contact your Elavon representative.

© 2011 Elavon, Inc. All rights reserved. Elavon is a trademark in the United States and other countries. All features and specifications are subject to change without notice. 06/11 Rev A