The Payment Security Dilemma:

Securing Cardholder Data While Reducing the Costs of Compliance

Did you know that data breaches occur each year at businesses like yours? Are you doing all you can to protect your bottom line and business reputation?

Elavon is committed to cardholder data security and helping you avoid fines, fees, and other costs associated with a breach.

Elavon offers a portfolio of security solutions and services designed to help businesses secure cardholder data, and streamline the process of Payment Card Industry (PCI) compliance, all while protecting and guarding your brand reputation.

DATA BREACH COSTS CONTINUE TO INCREASE

Data security is an enormous global challenge. Cardholder data is particularly at risk from hackers and thieves due to its value and portability.

Are you doing all you can to protect your bottom line and reputation?

Despite security advances, criminals across the world seem to find more sophisticated and intrusive means of attacking point of sale devices, back-office systems and network data centers. These attacks have evolved over time from pulling card receipts out of the trash or skimming a limited amount of cardholder data to using complex malware and data sniffing technologies which have captured millions of cardholder records globally.

Elavon

Increasing Risks

The number of security breaches is increasing, with total payment card fraud approaching $14 billion in 2013.[1] The cost of U.S. payment card fraud grew by 29% to $7.1 billion in 2013.[1] The industries most severely impacted by costly data breached are those related to retail, food and beverage, and hospitality[3], which accounted for 64% of the compromises. Retailers were the most impacted with some large nationwide companies making headlines. Restaurants and hotels are a prime target as card transaction data typically "sits" within systems to accommodate adjustments (e.g., tips, incidental charges) without the need for the actual card to be re-presented – making the information easier to capture.

The financial impact of data breaches can be severe.

For one major retailer suffering an extensive security breach, the total cost of the incident could reach $680 million[4]. One recent study found that 43% of consumers would avoid shopping a retailer that had been breached, and another 31% of shoppers will spend less at a breached retailer's stores. One recent study found that 69% of consumers would be less inclined to do business with a breached organization.[6] Other costs associated with breaches include: fines for non-compliance, notification, call center and credit monitoring costs, costs associated with forensic investigations, reputational damage, and the negative impact on consumer trust.[5] The forecasted average losses for breaches vary by number of cards compromised. For example, for smaller business, the forecasted average loss for a breach of 1,000 records is between $52,000 and $87,000. For larger businesses, the forecasted average loss for a breach of 1,000,000 records is between $892,000 and $1,775,000.[2]

PCI Compliance Guidelines

Fortunately, the payment industry has made significant strides in responding to security threats, with the founding of the PCI Security Standards Council and release of the first set of PCI standards and practices 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 security best practices developed to help those businesses which accept electronic payments to proactively protect their customer account data. The standards require maintaining a secure network, implementing internal controls and performing regular testing. As the experts on the Council identify new types of attacks, updated standards are released to help ensure businesses keep their security precautions up to date.

Potential Vulnerabilities

There are three potential points of risk across the lifecycle of a payment transaction

CARD IN USE – while being used throughout an enterprise for card present/card not present transactions, post-authorization, card on file adjustments, analysis and reporting

PAYMENT IN PROCESS – from the earliest point of entry in the data stream and while traveling to and from a gateway or processor

DATA AT REST – as a batch awaiting settlement or stored within a system

Top Priority

With the increasing risks and costs associated with payment security and PCI compliance, there is now broader adoption of EMV, encryption and tokenization solutions to remove cardholder data from their unguarded environment. These solutions enable a business to streamline the process of PCI compliance while reducing expenses associated with the security effort. Solutions that effectively remove cardholder data from the organization's processing environment have been shown to significantly reduce the complexity of PCI compliance audits, which vary widely in costs, time and resources depending on the organization's transaction volume and infrastructure.

[1] The Nilson Report, BI Intelligence. [2] Verizon 2015 Data Breach Investigation Report
[3]2014 Trustwave Global Security Report. [4]www.minnpost.com/glean/2013/12/one-estimate-cost-target-data-breach-could-hit-680-million.
[5] Verizon 2015 PCI Compliance Report. [6] Radius Global Market Research, Quirk's Marketing Research Review, June 2014

A Comprehensive Approach to Payment Security

Experts agree that securing your business is best achieved with a multi-layered approach, as there's just not a one-size-fits-all solution.

EMV "SMART CARD"

EMV (an acronym of Europay, MasterCard® and Visa®) is a global standard for payment cards using chip technology to authenticate the card and potentially the cardholder and reduce potential fraud at a physical point of sale. While traditional magnetic-stripe cards can be copied ("skimmed") relatively easily with inexpensive skimmers, chip technology assigns a dynamic value for each transaction, making cardholder data virtually impossible to skim.

EMV cards and EMV terminals have become the norm across most of Europe, and are now available in the U.S. from leading providers. The appeal of chip cards for consumers centers on their greater physical control of their card and the increased integrity EMV cards provide. Portable EMV devices are brought to the consumer, who inserts their card into the device to initiate the transaction, in much the same manner as an ATM machine works. With the card in their possession at all times, consumer satisfaction and confidence are both increased. It's an ideal solution for restaurants, retail and a wide variety of industries. EMV offers protection from the liability of various payment card fraud scenarios when a business processes the payment using an EMV terminal.

TOKENIZATION

Tokenization converts or replaces cardholder data with a unique token ID and stores the original data and token algorithm in a centrally-located, secure data center. It eliminates the possibility of having real card data stolen because the token is used in place of an actual account number. The token remains within the POS system and is called up (instead of the account number) to perform purchase adjustments, add new charges or perform other transactions.

Tokenization is well-suited for card not present environments (mobile, ecommerce) where payment credentials are stored. Tokenization also works well for businesses like hotels that often temporarily store transaction data, before submitting for processing or for health clubs, utilities and other businesses that process recurring transactions.

ENCRYPTION

Encryption encrypts the card data at the earliest point of entry to protect it as it travels across various systems and processing networks. Sophisticated algorithms render card data unreadable to anyone that gains access to it through hacking or skimming. A robust encryption solution protects data the instant a card is swiped or keyed on a terminal and keeps it encrypted until the data has traveled to a centrally-located secure data center for decryption and processing.

Encryption is ideally suited for any businesses that processes card present transactions.

Elavon Can Help Protect Payment Data and Your Bottom Line

The process of securing cardholder data and maintaining PCI compliance requires the right combination of security solutions tailored to your business operation. To address these challenges, organizations need a comprehensive solution that protects data at every phase within the transaction lifecycle – Card in Use; Payment in Process and Data at Rest.

Elavon has a long-standing commitment to protecting our customers, and has invested in a proven portfolio of security solutions which help secure and safeguard cardholder data, streamline the process of PCI compliance and ensure business process continuity by:

- Removing actual card data from the payments stream
- Utilizing EMV, encryption and tokenization to protect card and payment data across the transaction lifecycle.
- Integrating terminals supporting EMV and encryption with leading POS/PMS systems
- Ensuring the continuity of existing business processes requiring use of card data
- Reducing the costs and complexities of PCI compliance

When it comes to your customers' security, rely on an expert. Backed by U.S. Bank, Elavon offers 20 years of global payment processing and gateway experience. Our knowledgeable team of security professionals can guide you in making wise investments in data protection.

Contact Elavon today at 1-866-548-6826 to learn more about Elavon's payment security solutions.

Elavon