VALUED
MERCHANT SERVICES

PCI DSS and Handling Sensitive Cardholder Data—Why You Care

The cost of Payment Card Industry Data Security Standard (PCI DSS) compliance is vastly underestimated—but maybe not as understated as the tangible and intangible costs of a data breach.

Every merchant that accepts payment cards has a cardholder data environment (known as CDE, or the computer systems and applications that use or store sensitive card data) that comes under the purview of the PCI DSS. It’s possible to limit—and even shrink—the scope of the CDE in order to reduce or minimize the merchant’s PCI burden.

Table of Contents

Executive Summary

Merchants that accept debit, credit and prepaid cards are acutely aware of an additional burden placed on their businesses starting in 2006. This is the year that the Payment Card Industry Security Standards Council (PCI SSC) began publishing stringent, resource-intensive requirements concerning the security of handling and storing sensitive cardholder data. Since then, merchants have collectively spent in excess of $1 billion on compliance with the PCI DSS as part of their security programs.[1]

PCI DSS compliance includes a long list of requirements and is a significant responsibility for businesses of all sizes. The security requirements cost the largest merchants (Level 1), on average, $2.7 million, according to the analyst firm Gartner Inc. Even small merchants (Level 4) might have to spend several thousand dollars on the initial security assessment and new technology and security measures.[2] What's more, maintaining PCI compliance is a continuous process that requires constant vigilance and incurs ongoing costs. The penalties for noncompliance can be severe, including the merchant's loss of the ability to accept credit card payments and being audited and/or fined.

Still, the relentless drive to protect sensitive cardholder data is vital. Losses stemming from data theft are on the rise. According to the Ponemon Institute, the average cost of coping with a data breach in 2008 rose to $6.6 million—a 40 percent increase since 2006.[3] Moreover, the threats are evolving as organized thieves use ever more sophisticated techniques to hack into more merchants' systems to steal sensitive data. All parties involved in processing card transactions have an imperative to continually improve their data security techniques.

One of the top reasons a merchant is most likely to fail a PCI audit—and a leading factor in data theft—is the failure to adequately protect stored data. VeriSign Global Security Consulting Services, a division of security services vendor VeriSign, has conducted hundreds of PCI assessments in recent years. Of the merchant companies assessed by VeriSign, 79 percent were cited for the failure to protect stored data and thus failed their assessments.[4]

The challenge for merchants is finding and implementing a solution or set of solutions that adequately protects sensitive cardholder data at rest and in motion; that meets the requirements of PCI DSS; and that doesn't slow or impair business processes or decrease profits.

Key Takeaways

There are several key points for readers to take away and consider in the context of their businesses.

- → The cost of PCI DSS compliance is vastly underestimated. As the PCI DSS requirements grow more stringent, the cost of attaining, assessing and maintaining compliance grows larger each year. The cost burden falls largely on the millions of merchants that accept credit, debit and prepaid cards in the payment for goods and services. All merchants want to reduce the cost of PCI DSS compliance; some are beginning to do so by shrinking the footprint of the cardholder data environment (CDE)—the computer systems and applications that use or store sensitive card data. Reducing the CDE has the direct effect of lessening a merchant's time and money spent on PCI DSS compliance.
- → While the cost of complying with PCI DSS and the associated validation mandates are high, the cost of suffering a data breach can be much higher. Victim companies often pay out millions of dollars to contain or repair the damage resulting from a breach. That amount doesn't include the less-quantifiable, but just as critical, brand impairment that lowers the company's market value. The best defense against a data breach is a good offense with data-securing processes and technologies.
- → Of the 12 PCI DSS requirements, the one area that is most problematic and costly for many companies is requirement #3: protect stored cardholder data. Failure to adequately protect the sensitive data is a leading reason why companies fail their PCI assessments, as well as a leading factor in data theft or exposure. Reasonable attempts to protect the data can be costly, often because the data is used in business applications beyond the initial transaction. Spreading the data across more systems and applications increases the need for protective measures.
- → Merchants aren't expected to act alone in attempting to contain and even reduce the cost of their PCI DSS compliance. The card payment ecosystem includes many partners who can offer security solutions and assume some of the risks and responsibilities of protecting sensitive data.

What Is PCI DSS?

The PCI Security Standards Council contends that merchant-based vulnerabilities may appear almost anywhere in the card processing ecosystem. This includes point-of-sale (POS) devices, PCs or servers, wireless hot spots, Web-based shopping applications, paper-based storage systems and the unsecured transmission of cardholder data to service providers. Susceptibilities also can extend to outside systems operated by service providers and acquirers.

These vulnerabilities can, and often do, lead to the exposure or theft of sensitive cardholder data, especially at the merchant level. The Verizon Business RISK Team reports that payment card breaches were at the top of the list of all reported data breaches in 2008, far outnumbering other data-type breaches. What's more, fraudulent use of stolen card data was confirmed in 83 percent of the breach cases investigated by the Verizon team.[5]

Clearly, all businesses in the electronic payments ecosystem need strong data security measures to mitigate the risk of exposure. This is the premise behind the development of the PCI Data Security Standard. PCI DSS represents the best available framework to guide better protection of cardholder data. Until the PCI standards were published, merchants had little guidance about what specific actions to take to protect sensitive data. The situation was especially vexing for small merchants that lack in-house information technology expertise.

The PCI Data Security Standard

PCI DSS version 1.2 is the current global data security standard adopted by five of the payment card brands for all organizations that process, store or transmit cardholder data.[6] It consists of common sense steps that mirror best security practices. There are 12 general requirements with more than 200 specific sub-requirements that compliant businesses must meet.

PCI DSS represents the best available framework to guide better protection of cardholder data.

Goals	PCI DSS Requirements
Build and maintain a secure network	**1.** Install and maintain a firewall configuration to protect cardholder data **2.** Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	**3.** Protect stored cardholder data **4.** Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	**5.** Use and regularly update anti-virus software or programs **6.** Develop and maintain secure systems and applications
Implement strong access control measures	**7.** Restrict access to cardholder data by business need-to-know **8.** Assign a unique ID to each person with computer access **9.** Restrict physical access to cardholder data
Regularly monitor and test networks	**10.** Track and monitor all access to network resources and cardholder data **11.** Regularly test security systems and processes
Maintain an information security policy	**12.** Maintain a policy that addresses information security for employees and contractors

Figure 1: The goals and general requirements of the PCI Data Security Standard
Source: PCI Security Standards Council

PCI DSS version 1.2 is the current global data security standard adopted by the card brands that applies to all organizations—regardless of size or number of transactions—that store, process or transmit cardholder data.[7] Compliance with the PCI set of standards is enforced by the founding members of the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

The major payment card brands that established the PCI Security Standards Council have each defined four merchant levels, primarily based on the number of transactions a merchant processes in a year. The level definitions below are provided by Visa U.S.A. and MasterCard Worldwide.

Level	Definition
Level 1	→ Any merchant that annually processes 6 million or more Visa or MasterCard transactions → Any merchant who experienced a data breach
Level 2	→ Any merchant that annually processes from 1 million to 6 million Visa or MasterCard transactions
Level 3	→ Any merchant that annually processes from 20,000 to 1 million Visa or MasterCard transactions
Level 4	→ All other merchants

Figure 2: Typical merchant PCI DSS levels
Source: Visa U.S.A. and MasterCard Worldwide

The merchant level, as defined by the major payment card brands, ultimately determines the type of compliance demonstration and the manner in which a merchant must validate adherence to the PCI DSS. For example, Level 1 merchants have the highest burden of proof of compliance, which includes an annual on-site assessment by a Qualified Security Assessor (QSA); a quarterly network scan by an Approved Scan Vendor (ASV); and an Attestation of Compliance. At the other end of the spectrum, Level 4 merchants have the lowest burden of proof, which typically includes the annual completion of a Self-Assessment Questionnaire (SAQ); a quarterly network scan (if required according to the SAQ); and any additional compliance requirements that may be set by the merchant's acquirer. Regardless of the burden of proof, all levels of merchants are expected to attain and maintain compliance with PCI DSS to reduce the likelihood of breaches involving cardholder data.

The Challenges of PCI Compliance for Merchants

The PCI DSS requirements have a tremendous impact on the information technology systems utilized by every company in the card processing ecosystem. Compliance efforts have forced merchants to update existing systems and implement new hardware and software in order to segment networks, install firewalls, deploy data encryption technologies, implement data access controls, track and monitor access to data and networks, and much more.

The implementation and ongoing maintenance of the needed technology measures is expensive, and it continues to grow more expensive with time. According to a 2008 survey by Gartner Inc., Level 1 retailers reported spending an average of $2.7 million on PCI compliance, excluding the costs of PCI assessment services. That number compares with an average of $568,000 reported by Level 1 merchants in a fall 2006 Gartner survey. Also, Level 2 merchants reported spending $1.1 million on PCI compliance, as opposed to an average spending of $267,000 reported in fall 2006. Altogether, Level 1 and Level 2 U.S. merchants' spending to protect cardholder data and become PCI compliant increased nearly fivefold during the past 18 months, according to the Gartner report.[8]

Despite the expenditures, many Level 1 and Level 2 companies are still struggling with PCI and are coming to realize that the cost of PCI compliance is vastly underestimated. One reason for the initial misjudgment on cost is that merchant companies don't realize the full impact of PCI DSS requirement #3: protect stored cardholder data, until they fully understand the scope of where cardholder data is stored and how it is used.

Further complicating the matter, merchants are required to demonstrate on an ongoing basis that they have the proper controls in place to protect the data. For a Level 1 merchant, the scope (and cost) of an audit can be huge. What's more, a merchant may need to satisfy different compliance reporting requirements for each card brand the merchant handles, even though the card brands all mandate compliance to the same PCI DSS requirements. This further drives up the cost of validating PCI DSS compliance.

The Consequences of Noncompliance

Considering all the money spent by merchants, and all the hoops they jump through to comply with PCI DSS, it's important to remember that PCI compliance is not mandated by any law or government regulation. Rather, compliance is a contractual obligation. A merchant's failure to comply with PCI DSS—in other words, a breach of contract—can result in monetary fines and/or the loss of the privilege to accept payment cards. Since few merchants are willing to forgo accepting third-party credit and debit cards and operate on a cash-only basis, there seems to be little choice other than making the effort to comply with PCI DSS.

Many companies are still stuggling with PCI and are coming to realize that the cost of PCI compliance is vastly underestimated.

Just how serious is the threat of fines by the card brands? According to Gartner, "8 percent of retailers have been fined for failing to comply with PCI, while 22 percent have been threatened with fines for their non-compliance."[9] To minimize the likelihood of noncompliance, Gartner recommends, "Security audits should be conducted continuously or as frequently as possible, and not be limited to what's required by PCI."[10]

Noncompliance raises more than the threat of fines or loss of card privileges; it raises the specter of poor corporate governance—a charge that no board of directors wants to face. Therefore, many progressive companies view PCI compliance not merely as an obligation, but as an opportunity to develop processes and capabilities that improve their business performance in multiple areas, in addition to providing better protection for cardholder data. The Aberdeen Group reports that companies that are rated as "best in class" in PCI compliance follow the security standards in order to "protect the organization and its brand."[11]

Increasing Threats and Costs—Obstacles to Secure Transaction Processing

What Are the Risks From Evoloving Data Threats?

Despite the billions of dollars that merchants have already spent toward improving cardholder data security, serious threats from data breaches still exist, leading to business risks. Consider these possible risks that result from the exposure of sensitive data:

Risk	Outcome
Losses from fraud	Banks and payment processors may reclaim losses they sustain as a result of a merchant's data breach
Expenses for credit monitoring	Customers whose data is stolen may be entitled to credit monitoring for at least a year
Fines by card brands	Card companies may issue fines for PCI DSS noncompliance and prohibited data storage practices
Remediation costs	Capital expenditures may be necessary to replace or upgrade compromised hardware, software, applications and communications
Brand damage	Public reporting of a breach often is required by law, making it impossible to escape widespread bad publicity and loss of confidence in the merchant's brand
Expense of forensic examination and in-depth PCI audit	Depending on the extent of a breach, a forensic investigation could take months with very high costs

Ability to service or acquire customers	Business processes could be sufficiently interrupted to make it difficult or impossible to conduct "business as usual"
Potential lawsuits	Merchants who have experienced a breach have faced lawsuits from customers, financial institutions, ISOs, payment processors, card brands, state attorneys general and more
Drop in market capitalization	When financial damages reach a high enough point, a merchant's stock value and overall market capitalization can drop

Figure 3: The business risks resulting from a data breach

As a stark example of how a data breach can harm a business, a review of the January 2007 disclosure of a data breach at a well-known discount retailer reveals the following ramifications:[12]

- The company filed a report with the Securities and Exchange Commission, acknowledging that 45.7 million credit card and debit card records were stolen from its computers. Subsequent court filings in a case brought by banks against the retailer say the number of accounts affected by the thefts topped 94 million, up considerably from the 45.7 million account numbers initially thought to be compromised.
- The retailer incurred more than $550 million in expenses, which included fines, restitution for damages, security remediation, fraud losses and more.
- It experienced a 7.5 percent decline in its stock price and a $1 billion loss in market capitalization.
- It took the company more than 18 months to recover from the breach—and that doesn't include the intangible brand damage that still lingers.
- The company name will forever be linked with one of the most extensive (and expensive) data breaches in history.

But large companies like this international retailer are not the only ones at risk. Fraud attacks are happening down market, as well, to smaller merchants that perhaps have not hardened their systems yet. Although a thief may find the quantity of data that can be stolen from a smaller merchant is low, the merchant will find that loss to be just as devastating to his business as the 94 million stolen records were to the international discount retailer.

The Cost of Data Breaches

The cost of each data breach is different, of course, depending on how many sensitive records were compromised, and whether or not the information is used to commit fraud. Every company suffering a breach incurs a financial impact—some reaching astronomical numbers. There may be direct costs associated with customer notifications, remediation services for victims, a forensic examination, fines, lawsuits, and new or updated computer systems. Indirect costs that are harder to quantify may include loss of customer confidence and brand value.

For several years, the Ponemon Institute has measured the costs of data breaches to help companies better understand their business risks. In its study[13] of 43 companies that suffered a data breach in 2008, Ponemon found the total cost of coping with the consequences rose to an average of $6.6 million per breach, up from $6.3 million in 2007 and $4.7 million in 2006. The cost per compromised record in 2008 rose 2.5 percent over the year before to $202 per record, according to the study. The retail industry fared a bit better in 2008, with the average cost per compromised record being $131. That doesn't sound like much until you consider the 94 million records of the January 2007 breach discussed previously.

The IT Compliance Group reports that companies that have suffered the loss or theft of sensitive data have financial outcomes that include an average of 8.1 percent customer defections; 8.0 percent revenue decline; and 8.0 percent decline in stock price.[14]

Breaches involving payment card data far outnumbered breaches of any other data type in 2008. Nearly 80 percent of the incidents investigated by the Verizon Business RISK Team involved the loss of sensitive cardholder data.

Even a suspected breach can have a financial impact on a company. In an April 2009 article entitled, "The Real Cost of Data Breach,"[15] Robert Halsey, president of Royal Services Group Ltd., points out that an actual data breach doesn't even need to occur in order to cost a Level 4 merchant tens of thousands of dollars. "Once a merchant is even suspected of a breach, a team of PCI DSS certified forensics security examiners swoops in to review and inspect its business practices. This examination can take anywhere from a few days to several weeks, depending on the complexity of the systems involved," writes Halsey. He further says, "That means that for a minimum of several days, your business is brought to an absolute standstill while the examiners comb through your policies, records, computer and phone systems, and employees—and eat away at your productivity, sales and profits. And, as if that's not enough, at the end you'll have to pay the costs of the forensic examination, whether there was an actual breach or not: somewhere between $8,000 and $20,000 if you're a Level 4 merchant."

There is one more "cost" of a data breach: any size merchant that experiences a breach may be automatically escalated to the status of a Level 1 merchant in terms of the burden of proof for PCI DSS compliance. This means that even a very small merchant can be required to contract the services of a QSA to conduct a thorough on-site assessment every year. Such a requirement can be a significant financial burden for a small company.

The Common Causes of Data Breaches

From 2002 through 2008, the forensic investigators of the Verizon Business RISK Team conducted more than 600 investigations of breaches or suspected breaches of all types of data in all types of industries. The team's most recent insights were published in the 2009 Data Breach Investigations Report to help the public understand some of the common causes and attack vectors, as well as the data types that are commonly compromised.[16] Here are some of the highlights of the report:

- As a percentage of caseload for the Verizon Business RISK Team, payment card breaches remain near the 80 percent mark and far outnumber the other data types. Payment card data breaches consume 98 percent of all records compromised in 2008. Fraudulent use of stolen card data was confirmed in 83 percent of Verizon's cases, and 91 percent of all compromised records were linked to organized criminal groups.
- 2008 was a record year for number of records compromised: 285 million, with 99.9 percent of the records compromised from servers and applications.
- Three-quarters of the 2008 breaches occurred in just three industries: Retail, Financial Services, and Food and Beverage.
- Of the organizations suffering payment card breaches within the Verizon caseload, 81 percent were found not compliant with PCI DSS or had never been audited. This status was determined by the victims' attestations or Qualified Security Assessors.
- In 66 percent of the cases, the breach involved data that the organization didn't even know was on the system.
- Data breaches often result from a combination of events rather than a single action. In a majority of the cases, some sort of significant error contributed to the breach; for example, not applying a

patch to a known vulnerability, or misconfiguring software or a device, thus allowing exploitation of the error. In most cases, the attacks were not complex and would likely have been prevented if basic security controls had been in place at the time of the attack.

- Three-quarters of the attacks weren't discovered by the victimized company; often it was law enforcement agencies or individual victims who pointed out the problem. Breaches go undiscovered and uncontained for weeks or months in 75 percent of cases.

Bryan Sartin is managing principal, Verizon Business Investigative Response. Sartin says the nature of the criminal attacks he has investigated over the years is changing. "Cybercriminals have become much more sophisticated in the last decade," according to Sartin. "At first we saw directed attacks against specific companies that processed lots of sensitive data—banks, ATM operators, data processing companies. Then we observed a shift toward fully random attacks using botnets, SQL injections, authentication bypass and scans for vulnerabilities. Just recently, the criminals have shifted techniques again to pursue softer targets like data in transit or in the computer's running memory because it's not encrypted."[17]

A look at some of the recent breaches of merchant organizations shows that common mistakes or vulnerabilities contributed to or are suspected of contributing to the breach.

Breach/Date Reported	Known or Suspected Contributing Factors
International Discount Retailer January 2007	The company had an outdated wireless security encryption system and failed to install firewalls and data encryption on the computers using the wireless network. Thieves accessed the streaming data between hand-held price-checking devices, cash registers and the stores' computers. All told, approximately 94 million credit and debit accounts were compromised.
Midwestern Outdoor Gear Retailer September 2007	A computer containing the credit card information for customers who shopped at a specific store between July 2002 and June 2007 was lost or stolen. 112,000 credit card numbers and 10,000 transaction records were on the computer.
Global Electronics Retailer February 2007	A store employee used a skimming device (a hand-held credit card reader) to capture the card data of approximately 4,000 accounts. She sold the data to an outside party.
Northeastern Theater Box-Office Operator Januray 2009	This theater box-office operator compromised 60 customers' credit card data when an outside contractor replaced a Web server. Some cards were later used fraudulently.
Mid-Atlantic Restaurant Chain November 2008	A compromised POS system is suspected as the vector for the theft of customers' debit and credit card information that resulted in the fraudulent use of some of the cards.
Canadian Direct Marketing Company November 2008	A former employee is suspected of stealing a backup tape containing sensitive personal information including credit card data of 3.2 million customers. Though the data on the tape was encrypted, the tape also contained the means to decrypt the data.
Northeastern Supermarket Chain March 2008	Malware was surreptitiously installed on the servers of almost 300 stores.[18] When customers swiped their credit cards, the malware intercepted the data as it was being transmitted from the stores' POS systems to authorize transactions. The malware then forwarded the stolen card numbers and their expiration dates to an overseas destination. As many as 4.2 million credit and debit card numbers were stolen.
National Restaurant Chain September 2007	Hackers used false credentials to gain remote access to POS servers and installed packet-sniffing software on the servers. The software captured unencrypted Track 2 data as it was transferred from compromised POS servers to a central system for transmission to the payment processor.
New England Theater Operator December 2008	Hackers accessed this movie theater's server in an unknown fashion and stole customers' credit card data. Some of the data was used for fraudulent transactions.

Figure 4: Contributing factors to known data breaches
Sources: DataLoss DB - http://datalossdb.org and Privacy Rights Clearinghouse - http://www.privacyrights.org

Many of these breaches most likely would have been prevented with the implementation of security measures specified in the PCI DSS requirements. At the very least, the impact of the breaches could have been minimized with the use of technologies such as data encryption and/or tokenization that render the sensitive data useless to thieves.

Containing—and Reducing—the Burden of PCI DSS

How the Cardholder Data Environment Impacts PCI DSS

According to VeriSign, the leading reason why companies fail their PCI assessment is the failure to protect stored cardholder data.[19] This comes as little surprise; the charge to protect such sensitive data is quite a broad challenge. Not only is cardholder data used to authenticate a transaction, but it is also often used for settlements, reconciliation and chargebacks, as well as in other business processes such as loyalty rewards programs, marketing, sales auditing and loss prevention. It's possible for cardholder data to be used far and wide throughout a merchant company—often without the chief information security officer's knowledge. For example, VeriSign cites instances from its PCI assessments where sensitive cardholder data has been found in spreadsheet applications on workers' notebook PCs. When data is used in so many places and so many ways, the challenge to secure it grows exponentially.

By definition, every computer system and filing cabinet, along with every application, that uses or stores sensitive card data is part of the overall cardholder data environment, or CDE. A company's entire CDE is "in scope" for PCI DSS compliance. Even if sensitive data is encrypted within the CDE, it is still within scope of PCI DSS requirement #3: protect stored cardholder data. As cardholder data is used beyond the POS and for more purposes beyond transaction authentication, the CDE grows, and likewise PCI DSS compliance and validation grow more complex and costly.

When merchants conduct their initial appraisal on the resources needed to achieve PCI DSS compliance, they frequently underestimate the extent of the CDE. Indeed, in many cases it's not known that actual cardholder data is used in various business applications until the first thorough PCI DSS assessment is conducted. (Recall the finding from the Verizon Business RISK Team that in two-thirds of the cases of data breaches, the breach involved data that the organization didn't know was on the compromised system.) When the data is discovered, the scope of the CDE grows to incorporate the data's host systems and applications, and the requirements and costs to meet PCI DSS grow as well. For example, data encryption may need to be employed on a tape storage system utilized by the marketing department, which uses cardholder data to evaluate marketing campaigns. Even though the tape storage system is not connected in any way to the POS system, it still holds data that is required to be protected under PCI DSS.

It's Possible to Limit—Even Shrink—the CDE

Every merchant that accepts payments cards has a CDE that comes under the purview of PCI DSS. The extent of that CDE is within the hands of the merchant. It's possible to limit—and even shrink—the scope of the CDE in order to reduce or minimize the merchant's PCI DSS compliance and validation burden. There are numerous ways to do so, as described below.

For example, merchants can restrict the use of cardholder data to only those applications directly pertaining to payments: transaction authentication, daily settlements, chargebacks, add-ons for items such as gratuities or recurring payments, and so on. Such restrictions can help limit the environment of the data to the POS system, related applications and a storage system. The specifications of PCI DSS 1.2 provide guidelines on how to secure this rather limited CDE.

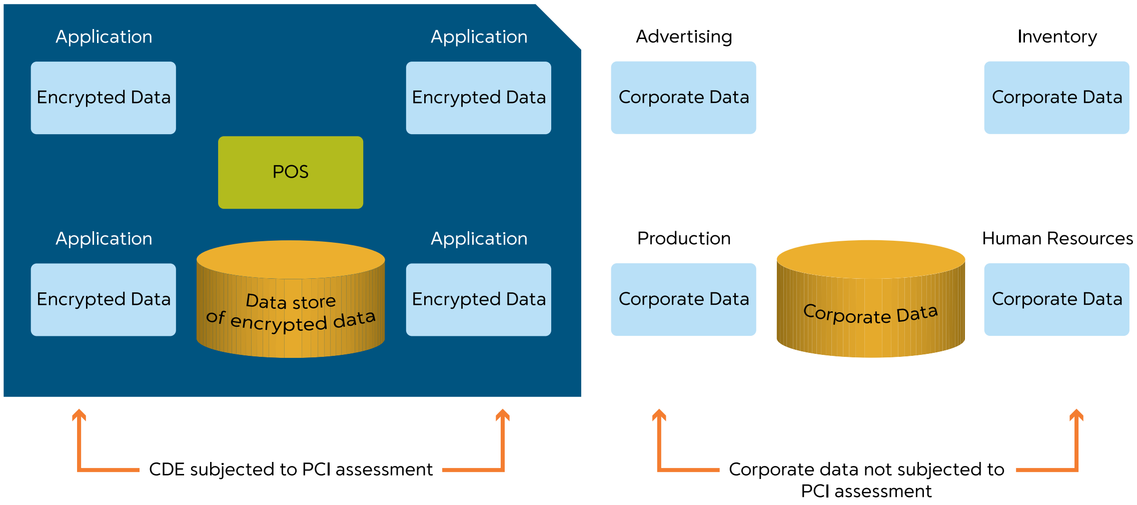

Figure 5: The CDE includes business applications that use cardholder data

Each business application that uses the cardholder data pushes the boundary of the CDE outward. That is, these applications and their related storage and data flows are now in scope for all PCI DSS assessments. But what if these applications could function exactly as they need to without the use of actual cardholder data? What if some representation of the cardholder data would act as a suitable stand-in? This is the principle behind the up-and-coming technology called tokenization.

In the process of tokenization, a credit card is used in a transaction and, once authorized, the cardholder data is sent to a centralized and highly secure server called a "vault." Immediately after, a random unique number is generated and returned to the merchant's systems for use wherever the cardholder data would be used. Essentially, credit card data has been removed from various business applications and replaced with a token. The token can be used by an authorized application to retrieve the stored cardholder data if necessary; otherwise, the business application simply uses the token instead of the cardholder data.

There are two significant advantages of this approach. First, the token has no meaning whatsoever to a hacker who might siphon it from a server or application, thus dramatically reducing the impact of a data breach. Second, the business application using the token data is not included in the CDE, since there is no cardholder data present. Merchants that replace cardholder data with tokens in all their business applications can significantly reduce the scope of the CDE, and subsequently reduce the scope and cost of PCI DSS compliance and assessment, as shown in Figure 6 on the following page.

Further benefit is achieved if the merchant outsources the data vault to a third party. Removing the data vault from the CDE—and handing the responsibility (and liability) for it over to the third-party service provider—even further shrinks the environment that is subject to PCI compliance.

Many industry experts believe that up-and-coming techniques and technologies (such as tokenization) offer the promise to reduce the scope of the CDE in far more extensive ways than current solutions, allowing potentially significant savings to merchants striving to meet PCI DSS requirements.

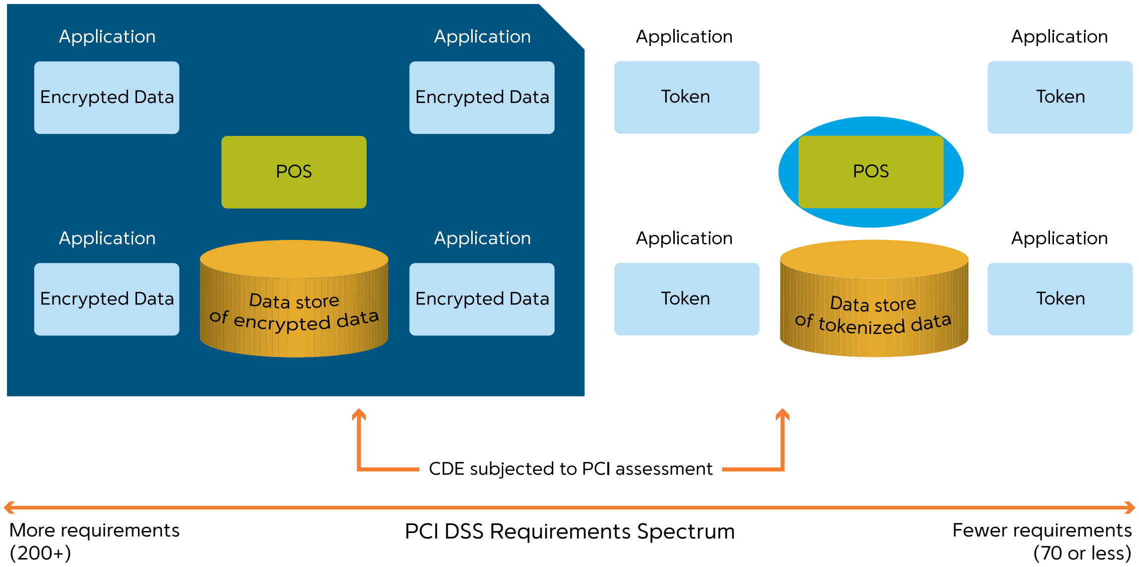

Figure 6: CDE scope reduction through the use of tokenization

Conclusion

PCI DSS compliance is growing more burdensome every year. As new threats to data security emerge, businesses are forced to apply more security techniques to attempt to stay a step ahead of cybercriminals and to plug newly identified vulnerabilities. The cost to attain, maintain and verify PCI DSS compliance is skyrocketing. Thus, all businesses in the card payments ecosystem have a vested interest in implementing long-term enhancements to data security and reducing the scope of the cardholder data environment.

Merchants don't have to do this alone. The end-to-end card payment process includes many participants—acquirers, ISOs, payment processors, card networks, etc. Merchants can look to these allies to assist with cardholder data security, and in the process, help reduce the burden of PCI DSS compliance.

First Data brings a wealth of PCI DSS knowledge to the table, along with a range of solutions that help keep data safe, meet the requirements of PCI DSS, help save money and support a merchant's critical business processes. First Data encourages all merchants to learn more about PCI DSS compliance, and to develop and implement a strategy to reduce and protect the cardholder data environment—or the ramifications of a breach could become a reality.