PCI DSS Compliance Overview

A compilation of Braintree blog posts

Braintree™
PAYMENT SOLUTIONS

Braintree™
PAYMENT SOLUTIONS

Table of Contents

I. PCI Compliance Overview

PCI DSS Compliance is an industry-mandated security standard that applies to all businesses that handle, process or store credit cards. There are 12 core requirements and roughly 250 controls, but as an oversimplification it boils down to three things: 1) all merchants, regardless if credit card data is stored, must achieve and maintain compliance at all times (all deadlines have passed); 2) merchants cannot store certain credit card information including CVV2, CVC2 and CID codes (three or four-digit numbers), track data from the magnetic strip or PIN data; 3) if permitted credit card information such as name, credit card number and expiration date is stored, certain security standards are required. A number of recent high profile breaches have been raising awareness and risks associated with PCI Compliance.

The motivation to become compliant

The major credit card companies have provided both carrots and sticks in order to compel merchants to become and maintain compliance. The incentives include 'safe harbor' from certain penalties and fines if a merchant is compliant *at* the time of breach. Without compliance, if a merchant is breached and has credit card information stolen, depending on the size of the breach, PCI related fines can be as high as $500,000 per incident. In severe cases, merchants can even be given the 'Death Penalty,' preventing them from accepting credit cards. In all, depending on the number of cards stolen, merchants are estimated to spend between $90 and $302 *per record* (see graph below).

II. The Payment Card Industry Data Security Standard (PCI DSS)

What is PCI DSS?

It's a comprehensive security standard that establishes common processes and precautions for handling, processing, storing and transmitting credit card data.

Who created it?

While Visa and MasterCard originally developed it, as of September of 2006 American Express, Discover, JCB, MasterCard and Visa jointly formed the PCI Security Standards Council.

Why was it created?

It was created in response to a spike in data security breaches over the last few years. A large number of both small and large businesses have been breached including TJX, Bank of America, Citigroup, BJ's Wholesale Club, Hotels.com, LexisNexis, Polo Ralph Lauren and Wachovia.

Who's at risk?

Any business that processes, transmits, or stores credit card information. While the publicity of security breaches has recently been focused on larger companies, Visa reports that the majority of breaches are occurring at small businesses.

What are the 12 mandated security requirements?

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored data
4. Encrypt transmission of cardholder data and sensitive information across public networks
5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications
7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security

What credit card information can and cannot be stored?

	Storage Permitted	Protection Required
Cardholder Data		
Account number	✓	✓
Cardholder name	✓	✓
Expiration date	✓	✓
Service Code	✓	✓
Authentication Data		
Magnetic strip	✗	n/a
CVV	✗	n/a
PIN data	✗	n/a

How much does it cost to become compliant?

It depends on business type, credit card processing and storage practices and existing IT environment. Read here for a more complete overview.

What do merchants have at risk if credit card information is breached?

Fines up to $500,000 per incident
Remediation costs estimated at $90 to $302 per record
Potential customer lawsuits
Company reputation and brand damage

Figure 1 The Cost Of A Breach, Broken Out For Three Sample Companies

		Cost per record		
Category	Description	Company A: Low-profile breach in a nonregulated industry	Company B: Low-profile breach in a regulated industry	Company C: High-profile breach in a highly regulated industry
Discovery, notification, and response	Outside legal counsel, mail notification, calls, call center, and discounted product offers	$50	$50	$50
Lost employee productivity	Employees diverted from other tasks	$20	$25	$30
Opportunity cost	Customer churn and difficulty in getting new customers	$20	$50	$100
Regulatory fines	FTC, PCI, SOX	$0	$25	$60
Restitution	Civil courts may ask to put this money aside in case breaches are discovered.	$0	$0	$30
Additional security and audit requirements	The security and audit requirements levied as a result of a breach	$0	$5	$10
Other liabilities	Credit card replacement costs. Civil penalties if specific fraud can be traced to the breach.	$0	$0	$25
Total cost per record		**$90**	**$155**	**$305**

42082 Source: Forrester Research, Inc.

Are their different requirements for large and small businesses?

Yes. Merchants belong to one of four levels that is determined by annual transaction volumes. These transactions volumes apply to the highest number of a single card type per year, e.g. a merchant doing 5,000,000 Visa and 2,000,000 MasterCard transactions annually, even though cumulatively equal 7,000,000, would qualify as Level 2.

Merchant level	Merchant definition	Requirement
Level 1	More than six million transactions annually across all channels, including e-commerce	Annual Onsite PCI Data Security Assessment and Quarterly Network Scans
Level 2	1,000,000 - 5,999,999 transactions annually	Annual Self-Assessment and Quarterly Network Scans
Level 3	20,000 - 1,000,000 e-commerce transactions annually	Annual Self-Assessment and Quarterly Network Scans
Level 4	Less than 20,000 e-commerce transactions annually, and all merchants across channel up to 1,000,000 VISA transactions annually	Annual Self-Assessment and Annual Network Scans

Definitions from above:

On-Site Security Audit

The audit must be completed by Level 1 merchants. Merchants can choose to complete the audit internally or hire an outside Qualified Security Assessor to complete the Report on Compliance (ROC). PCI Security Audit Procedures & Reporting

Self-Assessment Questionnaire (SAQ)

Initially the Council had a one size fits all SAQ but it proved too challenging and complicated for the different types and sizes of merchants. In February 2008, the merchant released four versions of the SAQ in an attempt to better accommodate merchant profiles. Here is a summary:

- SAQ A: Addresses requirements applicable to merchants who have outsourced all processing, transmission and storage of cardholder data.
- SAQ B: Created to address requirements pertinent to merchants who process cardholder data via imprint machines or stand-alone dial-up terminals only.
- SAQ C: Constructed to focus on requirements applicable to merchants whose payment applications systems are connected to the Internet.
- SAQ D: Designed to address requirements relevant to all service providers defined by a payment brand as eligible to complete an SAQ and those merchants who do not fall under the types addressed by SAQ A, B or C.

Network Vulnerability Scans

The PCI Standard requires merchants to scan all outward facing IP addresses. These IP addresses are not protected by a firewall and can be hacked through an open port. The SAQ identifies and mitigates risk from the inside (behind the firewall) while the IP scans identify and mitigate risk from the outside.

Validation Dates

The Card Associations have set specific dates for validation. Level 1 merchants were required to validate compliance by 9/30/2007, Level 2 by 12/31/07, and the Level 3 and 4 deadlines are processor/acquirer specific.

How to Get Started

1. Identify the individuals that will be responsible for PCI compliance in your organization and assemble a team that includes members from each area.
2. Determine your merchant level (1-4).
3. Determine which SAQ your organization will need to complete.

4. Evaluate whether your organization will try to achieve compliance internally or engage with a Qualified Security Assessor (QSA).
5. Engage with an Approved Scanning Vendor (ASV) to start the required external IP vulnerability scans.
6. Make sure that your organization has an Information Security Policy and that it is being enforced.
7. Immediately address any significant deficiencies discovered during the assessment or scan.
8. Retain record of self-assessments, scans, and follow-up activities. Be prepared to provide these documents upon request.

What should you do if breached?

In the event of a security incident, merchants must take immediate action to:
1. Contain and limit the exposure. Conduct a thorough investigation of the suspected or confirmed loss or theft of account information within 24 hours of the compromise
2. Alert all necessary parties. Be sure to notify:

•· Merchant Account Provider
•· Visa Fraud Control Group at (650) 432-2978
•· Local FBI Office
•· U.S. Secret Service (if Visa payment data is compromised)

3. Provide the compromised Visa accounts to Visa Fraud Control Group within 24 hours.
4. Within four business days of the reported compromise, provide Visa with an incident report.

Here is a step-by-step guide from Visa - *What To Do If Compromised*.

Additional resources:
A non-profit organization, RSPA produced a 12-minute video aimed at educating smaller restaurant and retail merchants about the risks associated with PCI Compliance.

III. The Risk and Cost of a Credit Card Breach

TJX is now the poster child for credit card data breaches. Starting in July 2005, hackers spent 18 months exploiting weak wireless network security outside of thousands of TJX owned stores and downloaded nearly 100 million credit card numbers and other personal information. TJX recently estimated that the breach will cost them $118 million. Others, such as Forrester, estimate it will cost them $1.35 billion after including legal fees, call center costs, regulatory fines, etc.

While TJX has received all the recent attention, breaches are occurring more often than many realize. The exact number is unknown because only 31 states currently have laws

requiring disclosure. One thing is for sure: if a business gets breached, the financial, business and PR risks are tremendous. A Forrester report determined that the cost *per breached record* will be anywhere from $90 to $305.

Figure 1 The Cost Of A Breach, Broken Out For Three Sample Companies

		Cost per record		
Category	Description	Company A: Low-profile breach in a nonregulated industry	Company B: Low-profile breach in a regulated industry	Company C: High-profile breach in a highly regulated industry
Discovery, notification, and response	Outside legal counsel, mail notification, calls, call center, and discounted product offers	$50	$50	$50
Lost employee productivity	Employees diverted from other tasks	$20	$25	$30
Opportunity cost	Customer churn and difficulty in getting new customers	$20	$50	$100
Regulatory fines	FTC, PCI, SOX	$0	$25	$60
Restitution	Civil courts may ask to put this money aside in case breaches are discovered.	$0	$0	$30
Additional security and audit requirements	The security and audit requirements levied as a result of a breach	$0	$5	$10
Other liabilities	Credit card replacement costs. Civil penalties if specific fraud can be traced to the breach.	$0	$0	$25
Total cost per record		**$90**	**$155**	**$305**

42082 Source: Forrester Research, Inc.

The profitable world of stealing credit card data

The spike in this type of criminal activity is attributable to the lucrative business of selling stolen credit card information. Depending on the quality, the selling price of a single record can easily be $100.

Criminals are using a host of tactics to steal credit card data. One of the most common methods is remote access to servers that house the data, like in the case of TJX. WEP 104-bit encryption can be cracked in under a minute on an 802.11g network by using active ARP-relay packet-injection techniques.

Another very common approach is "skimming", a practice through which an employee attaches an electronic reader to the point of sale machine to steal cardholder information including name, credit card number, and the CVV2 code (three or four-digit number on the front or back of the card). Employees have also been known to write down this information.

In ecommerce environments, cyber criminals are using SQL Injection, Cross Site Scripting (XSS), and Buffer Overflow attacks.

IV. PCI Compliance overview

The driving force behind the effort to secure all credit card data is the PCI Security Standards Council, which was founded by Visa, MasterCard, American Express, Discover and JCB. They have mandated that businesses meet 12 security requirements in order to protect cardholder data.

To provide proper incentives, the Card Associations have offered both carrots and sticks. As a carrot, merchants are offered protection from PCI-related fines, which can be as high as $500,000 per incident, if they are compliant at the time of the breach - something called Safe Harbor. As a stick, merchants can face the above-mentioned fines when breached as well as be fined for non-compliance. Some card brands have threatened to levy fines against larger merchants, up to $25,000 per month, until they obtain compliance.

To start the process of becoming compliant, a company should consider engaging a Qualified Security Assessor (QSA) who can advise regarding remediation and are approved to complete the official assessments for the Card Associations. There are fewer than 100 companies that offer these services. A few examples include Accuvant, Security Metrics, and Trustwave. The process of becoming compliant may take anywhere from 3 month to 2 years, depending on the business size and current IT and security infrastructure.

Taking matters into your own hands

A few things that can be done right away is making sure prohibited information is being purged after authorization. That information includes full track data (on the magnetic strip), CVV2, CVC2 and CID codes (three and four-digit codes) and PIN data.

If businesses need to store name, credit card number and expiration date, it needs to be secured either internally or stored remotely. Credit card tokenization, a remote storage technology, allows for a unique customer ID to be created for each record which is then used to remotely initiate transactions or change customer files without ever handling any sensitive credit card data.

Other simple ways to better protect from breaches include tightening remote access controls, changing wireless network security from WEP to WPA, properly configuring firewalls, changing vendor default passwords, and using encryption to transmit all sensitive data.

In summary

Regardless of a business's current situation, the cost of a breach can be enormous. TJX, a $17 billion dollar retailer will be able to weather the storm, but a smaller organization may not have the same financial depth, which means the consequences may be much more severe. So whether or not the required resources are available to pursue PCI Compliance and proper data storage, it might not be a bad idea to make it a priority in your organization.

V. The Cost of Becoming PCI Compliant

The cost of becoming PCI DSS Compliant depends on a number of factors including your business type, number of transactions processed annually, existing IT infrastructure, and current credit/debit card processing and storage practices. Gartner estimates that during 2007, the nation's largest merchants, classified as Level 1 (processing in excess of 6 million transactions of a single card type per year), will spend $125,000 assessing the scope of required PCI-related work and another $568,000 to meet the requirements. As an example, Robin Sidel and Pui-Wing Tam of the WSJ recently reported that Guitar Center, a national retailer of 210 stores, recently spent nearly $500,000 to become compliant.

Gartner also concluded that Level 2 merchants, those processing between 1 and 6 million annual transactions, will spend $105,000 to determine scope and another $267,000 for compliance. Level 3 merchants, processing between 20,000 and 1,000,000 e-commerce transactions, are expected to spend $44,000 assessing and $81,000 for compliance.

The costs associated with Level 4 merchants, those doing less than 20,000 ecommerce transactions or up to 1,000,000 non-ecommerce transactions, varies widely.

Only Level 1 merchants are required to have an on-site audit. Levels 2, 3 and 4 need to fill out the Self Assessment Questionnaire and sign up for a quarterly scan to check vulnerabilities on all outward-facing IP addresses. A rough estimate for the scans is $150 to $2,500 per IP address per year. Other costs may include software and hardware upgrades if information is stored in house. Gartner estimates that a company with 100,000 credit cards on file will pay $6 dollars in encryption costs per card. Alternatively, merchants can use technologies such as tokenization where the data storage is remote, which typically have per transaction fees instead of upfront costs.

All of these estimates exclude the cost of labor and the opportunity cost of pursuing other profit-making endeavors.

Smaller restaurants and retailers that only have a single terminal or POS system are still required to become compliant. Both need to fill out the Self Assessment Questionnaire, but the compliance process is usually much less involved. Merchants that are using POS systems to process credit cards need to make sure they are not improperly storing prohibited card data and need to verify that their vendor is PABP compliant (soon to become PA DSS). To verify that your POS system is not storing prohibited information and is compliant, see this updated list was published in November 2007. Some merchants such as Brad Friedlander, a restaurant owner in Cleveland with two stores, paid $50,000 on technology upgrades to become compliant.

Any merchant that accepts, stores, or processes credit card information is required to already be compliant. The Card Associations have determined specific dates about

when merchants need to validate compliance. Level 1 merchants were required to validate compliance by 9/30/07. Level 2 are expected to validate compliance by 12/31/07. Level 3 and 4 validation deadlines will come, but at this point they have been left up to the merchant's specific acquirer to be determined.

Not only is becoming compliant not optional, but Card Associations have threatened larger merchants with the imposition of monthly fines until compliance is obtained. They've also threatened to increase the cost of interchange, which would increase these merchants' processing costs. But perhaps most importantly, the Card Associations will levy fines and penalties if a merchant is not PCI Compliant at the time of breach. The fines can be devastating to merchants. I've written about two breaches, both of which had significant consequences. One merchant is large, the other is small.

Some merchants are frustrated about the PCI requirements, while others see them as basic security requirements that should already be in place. A common misconception is that compliance equals security, but a number of recent breaches have proven that not to be the case.

VI. HBR Case Study: How to deal with a credit card breach

In the September 2007 issue of the Harvard Business Review, Eric McNulty writes an article Boss, I Think Someone Stole Our Customer Data. This is a **must-read** for any executive or business owner whose company accepts credit cards. Mr. McNulty does a great job at clearly framing out PCI Compliance, data security, and potential responses and ramifications of a security breach.

The author included in the article four expert opinions regarding the case study. It includes James Lee, SVP of ChoicePoint; Bill Boni, Corporate Information Security Officer at Motorola; John Coghlan, former President and CEO of Visa USA; and Jay Foley, Executive Director for Identity Theft Resource Center. All offer valuable insights.