

The Smart Approach to PCI DSS Compliance

A Braintree Payment Solutions White Paper

By
Ben Rothke, CISSP, PCI QSA

Braintree Payment Solutions
802 West Bartlett Rd
Bartlett, IL 60103
www.getbraintree.com
(630) 540-1006

Table of Contents

Overview

3 What's at Risk?

4 Encryption

4 Outsourcing

The Smart Approach

5 Handling Credit Card Data

5 Storing Credit Card Data

Comparison

7 Security Comparison

8 Cost Comparison

9 Benefits of Braintree's System

Conclusions

About

Overview

PCI Compliance is an industry mandated security requirement for any business that 'handles, processes, stores, or transmits credit card data'.

There are 12 core requirements that break out into nearly 225 individual controls, and meeting all of those controls is an expensive and time consuming proposition. Gartner estimates that merchants will incur substantial costs assessing 'scope' and implementing required solutions.

Gartner Compliance cost estimates for Level 1-3 merchants

Assessment costs to determine scope	\$44,000 to \$125,000
System upgrades	\$81,000 to \$568,000

WHAT'S AT RISK (A LOT!)

Millions of customer data records have been compromised recently. To be exact, over 260 millions records in the last decade according to the [Privacy Rights Clearinghouse](#). The most notable of which was the high profile breach at TJ Maxx which has left little doubt that companies face significant risk in not becoming PCI compliant. In addition to the significant amount in fines from the card associations, TJ Maxx has incurred significant remediation costs. Fines can be as much as \$500,000 per incident for smaller companies and experts have estimated the cost of remediation to be roughly \$200 per breached record.

TJ Maxx, and their parent company TJX, violated some basic PCI tenets and its insecurity has had a direct negative financial effect. The company announced it took a \$12 million loss for their fourth quarter, equal to 3 cents per share, because of the more than 40 million credit and debit card numbers that were stolen from its systems over an 18-month period, making it one of the largest customer data breaches to date.

“Regardless of merchant size, there is no question that the stakes are high and compliance is necessary.”

The \$12 million in losses included costs incurred to investigate and contain the intrusion, improve computer security and systems, and communicate with customers, as well as technical, legal, and other fees.

The company also reported that it expected to continue to incur these types of costs related to the intrusion, totaling 2 cents to 3 cents per share, as well as battle federal, state and personal lawsuits.

Such breaches are precisely what PCI comes to prevent. Had TJX followed the principles of PCI and properly secured their systems, they would have seen a positive return on their investment, and saved the companies millions of dollars in fines and negative publicity.

And it is not just large companies that are at risk. Nearly 70% of all breaches are occurring at smaller merchants, who are less able to absorb the high financial cost associated with a breach. Regardless of merchant size, there is no question that the stakes are high and compliance is necessary.

ENCRYPTION

Achieving and maintaining PCI Compliance in-house

The traditional method of securing sensitive data has been through encryption, a process that locks access to data by making it readable only through specific knowledge about the coding, most commonly through a key.

Data can be encrypted using several different algorithms which vary in strength. With technology advancing, merchants have to stay ahead to ensure their data cannot be decrypted by hackers continuously working to break encryption algorithms.

While the locking up of the data is relatively easy, securely storing the keys so they are not lost, destroyed, copied or stolen is more complicated. NIST outlines recommendations for the proper management of keys (available online at http://csrc.nist.gov/groups/ST/toolkit/key_management.html). Merchants who encrypt data in-house must ensure everything from the proper storage and handling of keys to a viable system for updating and destroying keys to ensuring keys are only available to the right users. One misstep with the keys and the data could still be stolen by hackers or locked up forever. Though data is encrypted and in compliance with PCI DSS, the responsibility is only shifted from protecting the data to protecting the keys.

PCI OUTSOURCING

The trend in IT over the past decade has been to outsource. In fact, Gartner (*PCI Compliance Is Hard to Achieve but Worthwhile*, 4 May 2007) states outsourcing PCI data storage as a best practice. A compelling solution is to simply move your customer data from your insecure infrastructure to an outsourced secure infrastructure. Done right, an outsourced solution is more economical and secure than attempting to do things internally. Done wrong, which too many organizations have done, and your compliance problems are exacerbated.

In evaluating an outsourced versus in-house approach, most businesses make the common mistake of significantly underestimating the amount of time, money and effort that is required to achieve and perpetually maintain PCI compliance. It is important to find a long term solution that is cost effective, not resource intensive, and offers full security.

It is also important to note that securing credit card data internally via encryption is the hardest PCI requirement to meet. Gartner surveyed 50 US retailers asking them, "What part of the PCI standard has been the hardest for your organization to comply with?" An astounding 46% responded that encryption was the hardest. Gartner noted that the intricacies involved with application integration, key management, and other areas, make encryption a struggle.

"Outsourcing PCI data storage is a best practice"

Gartner also concluded that merchants *should not* be hesitant to spend money on data protection, as it costs substantially less to protect data than to suffer a data breach. This issue must be stressed as Gartner listed insufficiently protected stored data as the most-common noncompliance area.

BRAINTREE'S UNIQUE OUTSOURCED APPROACH

Braintree's solutions help merchants comply with the PCI DSS regulations for the *handling, storing, processing, and transmission* of credit cards, with very little to no impact to the merchant's regular operations and procedures. With Braintree, merchants are immediately able to reduce the number of required controls from 225 to less than 20. The following table shows the compelling differences between attempting to do it yourself and using the Braintree solution:

	Braintree deployed	In-house solution
Time to become compliant	30 to 60 days	6 to 18 months
PCI DSS controls to address	Less than 20	Over 200
Assessment costs to determine scope	\$0	\$44,000 to \$125,000*
Hardware/Software Upgrades	\$0	\$81,000 to \$568,000*
Ongoing Expenses	Fixed	Variable

*Gartner estimates merchant Level 1-3

HOW THE BRAINTREE SOLUTION WORKS

Braintree's solution addresses the two crucial components of PCI compliance by remotely *storing* credit card information in a Level 1 PCI compliant facility and preventing any *handling* of cardholder data. By addressing these two critical components, merchants can dramatically reduce time to compliance, reduce costs and increase security.

Handling of Credit Card Data

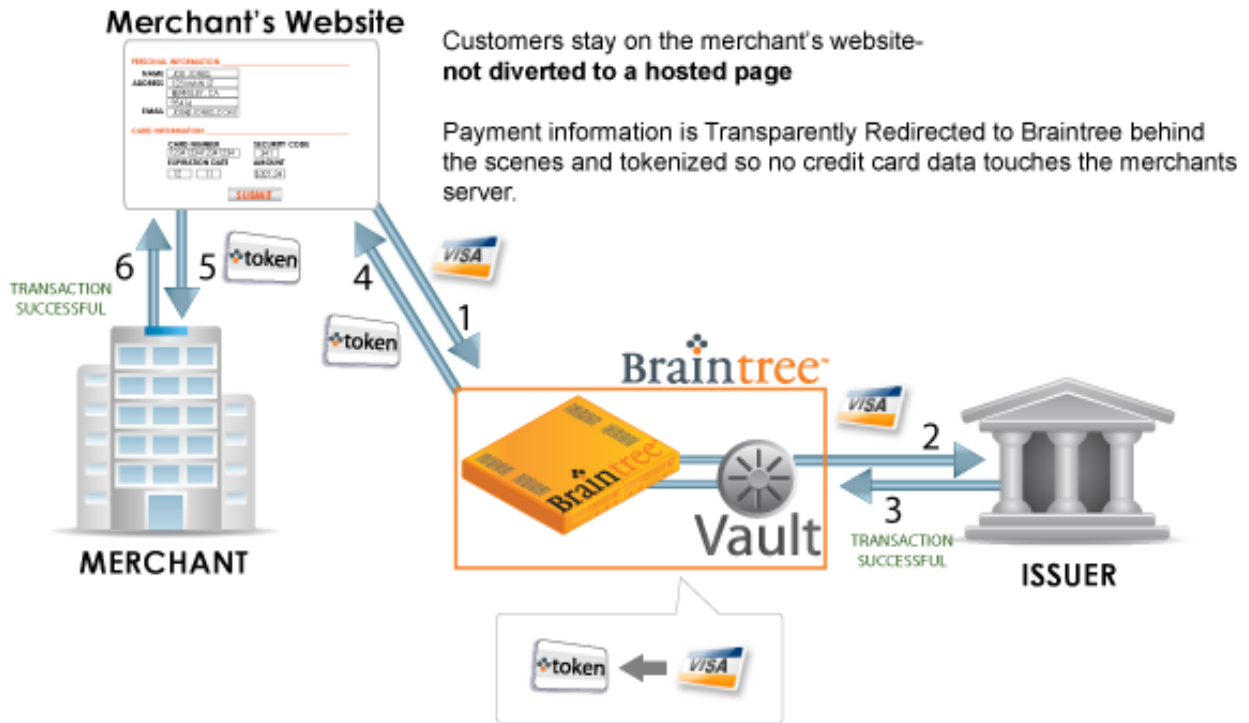
Braintree's **Transparent Redirect**, an innovative and powerful technology, allows merchants to accept payments via their website or over the phone without ever having to 'handle' sensitive card holder information. With Braintree, payments are accepted as before with the exception that no sensitive credit card data traverses the merchant's environment. Traditionally, the credit card data is collected by the merchant's server and then transmitted to the gateway. Braintree's pioneering technology allows merchants to send the data to Braintree's gateway directly from their ecommerce page, without affecting the user's experience.

Storing Credit Card Data

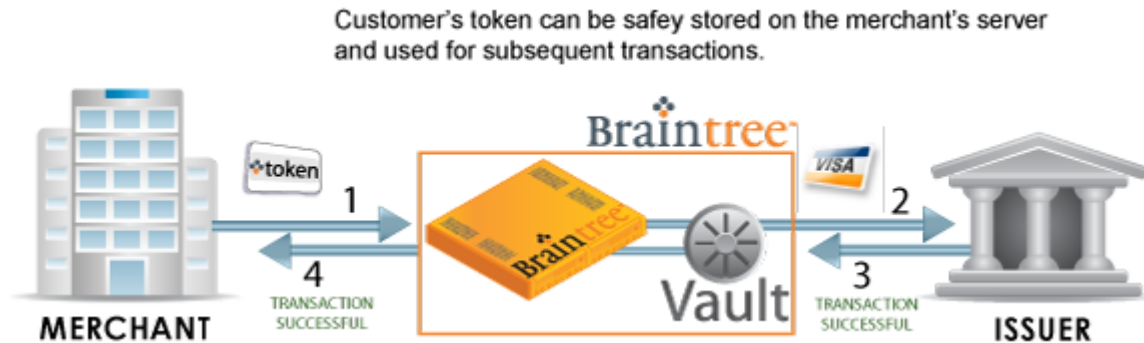
Braintree's **Vault** remotely stores all sensitive credit card information in a Level 1 PCI Compliant environment. A unique customer ID, in the form of a token, is returned to the merchant upon submitting sensitive credit card details to the Vault. Subsequent transactions can then be initiated remotely without ever handling any sensitive information. The unique customer IDs (tokens) can be stored on the merchant's server and are useless to criminals

Ecommerce example

Payment is accepted from the merchant's ecommerce website directly (Transparent Redirect) and tokenized (Vault) so the merchant is not exposed to full credit card information.

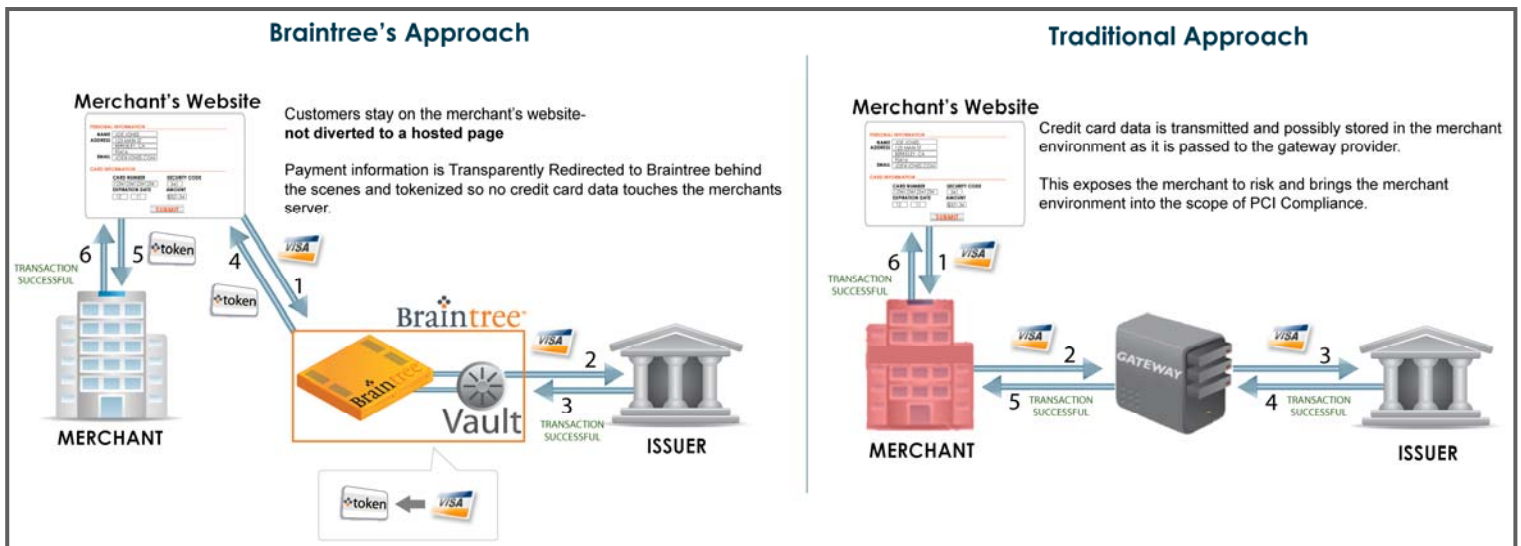


Merchants can store the tokens and use them to issue subsequent transactions, without the related PCI Compliance regulations.



Vault	Transparent Redirect
Allows repeat purchases without requiring payment information each time	Enables merchant to accept payments from customers without handling or storing cardholder data
Enables merchant to update, change, or delete customer data at anytime	Seamlessly integrates into existing infrastructure.
View and display customer transaction history and truncated credit card information	Incorporates innovative security technology.
Visa CISP compliant solution	Solutions are platform-agnostic. Use Ruby, PHP, ColdFusion, ASP.NET, Java and others.

SECURITY COMPARISON- BRAINTREE VS. IN-HOUSE SOLUTION



COST COMPARISON - BRAINTREE VS. IN-HOUSE SOLUTION

Let's take a look at the following hypothetical case study for a typical Level 3 merchant where the bulk of transactions are card not present (i.e., via website, phone, or mail order). Let's assume that this merchant processes 65,000 credit card transactions per year; 40,000 via its website and 25,000 via phone order.

To properly address PCI Compliance requirements, determine scope and map out a remediation plan, the following are typical and industry standard expenses though there costs vary based on a number of factors. (Note: Braintree's costs vary according to volume).

In-house			Braintree		
Set up Fees					
	Weeks	Total		Weeks	Total
PCI Environment Discovery & Initial Compliance Assessment			None	-	-
PCI QSA (Security Architecture Lead & PM)	4	\$28,000			
Engagement Manager (8 hours per week)	4	\$5,600			
PCI Gap Analysis & Remediation Planning					
PCI QSA (Security Architecture Lead & PM)	8	\$56,000			
Security Consultant (Security Policy Lead)	8	\$56,000			
Engagement Manager (8 hours per week)	8	\$11,200			
PCI Remediation Implementation					
PCI QSA (Security Architecture Lead & PM)	8	\$56,000			
Security Consultant (Security Policy Lead)	8	\$56,000			
Engagement Manager (8 hours per week)	8	\$11,200			
Other					
Encryption devices	1	\$15,000			
Hardware Security Module	1	\$7,750			
Additional Security Software	1	\$5,000			
Implementation	800 hrs	\$14,000			
Total		\$321,750	Total		\$0

Ongoing Charges			
Quarterly Scans	\$350	Monthly Service Charges	\$416
Annual software maintenance/upgrades	\$2,500		
Annual hardware maintenance/upgrades	\$2,500		
Annual Cost	\$5,350	Annual Cost	\$5,000

Three Year Grand total \$337,800

Three Year Grand total \$15,000

NOTE: Given the vast disparities between merchants, from the Fortune 50 to the corner deli, creating a comprehensive cost comparison is beyond the limited scope of this white paper. Nonetheless, the estimates here are based on a typical level 3 merchant.

BENEFITS OF BRAINTREE'S SOLUTION

The financial case is compelling. In addition to the cost savings, there are other areas where an outsourced solution is convincing:

Issue	Benefit
Shortened time to implement	Do it yourself time to implement PCI compliant solution - 6 to 18 months, Outsourced solution - 1-3 months
Flexibility	An outsourced solution makes MACD (moves, adds, change, deletions) of customer data relatively easy.
Security	Braintree's Vault provides greater security and significantly lowers the risk of a data breach due to its compliance with Level 1 PCI requirements.
Resource optimization	Braintree's solution optimizes the use of in-house resources by minimizing required hours
Experience	Braintree's extensive knowledge and technical capabilities can be put to use to manage your PCI data compliance process.

Once the Braintree solution is in use, all PCI data is encrypted. In the event that the data is intercepted, it is unreadable to the attacker.

Another benefit is the Braintree API (application programming interface.), a set of routines provided in libraries that extends the Braintree functionality. The Braintree API easily integrates into your application and cuts down on costly and often complex code recoding.

Conclusions

Deciding on an outsourced solutions provider is a major decision. Gartner notes that whether you process card payments in-house or use a third-party service provider to perform some of your work that handles credit card data, *you* are the party that is responsible for PCI compliance.

By using the Braintree solution to secure your PCI data, you can rest easy knowing that the security is there, as is the significant cost savings- which is an unbeatable combination.

Braintree's Vault with Transparent Redirect is a superior solution for PCI DSS Compliance.

About the author

Ben Rothke CISSP, CISM, PCI QSA (ben.rothke@bt.com) is a Senior Security Consultant with an international professional services firm and the author of [*Computer Security: 20 Things Every Employee Should Know*](#) (McGraw-Hill, 2006). He has written extensively about PCI for publications such as CIO, CSO, BizTech Magazine and Network World.

About Braintree

Braintree Payment Solutions is a leading provider of end-to-end electronic payment products and services. Braintree processes all forms of electronic payment transactions – credit, debit, electronic check, and electronic funds transfer. The company offers simplified PCI Compliance and credit card storage solutions, risk and fraud management, ecommerce solutions, and rate management. We're changing the industry one customer at a time and would invite you to experience the difference.

Visit us on the web at <http://www.braintreepaymentsolutions.com>