Reducing PCI Compliance Costs Through Outsourcing

Executive Summary

The annual costs for PCI compliance across multiple sites and web applications seems very excessive ($100k or more) and trying to reduce those costs in house will take a long time or require purchasing more equipment to segment the card holder environment. Outsourcing the hosting and maintenance of the card data can reduce the PCI scope of your organization by removing the card holder environment from the organization.

Introduction

Businesses that start growing and processing credit cards occasionally fail to secure their card holder data in a separate network space and once the business grows past a certain size, find it difficult to add the network segmentation, policies and update the applications processing credit cards as quickly as the regulatory body (Visa letter or other notification from an auditor or your merchant service company). For some businesses, trying to navigate the PCI compliance rules requires a new hire and then time to develop a final solution. If left unchecked, PCI can ban your business from processing a specific card type until the PCI Compliance is reached.

Problem Definition

After receiving a letter or notification regarding a PCI violation or that the card brand is auditing your systems, the IT department starts looking into the requirements for PCI and realize there is a lot of work to do across the organization becoming PCI Level 1, 2, 3 or 4 certified. The different levels define the number of Visa transactions processed in a year. Level 1 is over 6 million Visa transactions per year, Level 2 covers 1M-6M Visa transactions per year, Level 3 covers 20,000 to 1M Visa eCommerce transactions per year, Level 4 covers less than 20,000 Visa eCommerce transactions per year and all other merchants processing up to 1M Visa transactions per year.

After being notified, the leadership has realized new corporate policies will be needed, the IT department states new hardware and system costs will be needed, in-house software will need some redesign and all employees will need new yearly education – all creating a new overhead cost to accept credit card transactions.

Category	Typical Fees or Time	Vendor Responsible?	Corporate Responsible?
Auditor	2-3 months of time; $18,000	Yes	No
Auditor On-Site Costs	$500/day on site; 4-5 days	Yes	No
Penetration Test (External)	$15,000	Yes	No
Penetration Test (Internal)	$10,000	Yes	No
Firewall Segmentation & Quarterly Review	$80/hr for a consultant to assist with firewall; 30 hours = $2400; 1 hour per review	Yes	No
PCI Quarterly Scans	$1300/year	Yes	No

Patching Policy Validation	2-4 hours to month to validate and update systems	Yes	No
Writing/Review Policies	120 hours of work with a committee of various departments	Yes	No
Corporate Education of Credit Card Processing	$25-50/employee online education options	Yes	Yes
Firewalls & Anti-Virus Software	$20/seat and domain policy	Yes	No, less the employee accesses card data
Scanning for Rogue Wireless Access Points	2-4 hours per quarter	Yes	No
Scan for Unencrypted Card Data Quarterly within network	10 hours per quarter	Yes	No
If internally developed, software change control and review procedures. Education to be included	+ .2 development hour per change request	Yes	No
Separation of the Card Holder Data Network	Additional networking hardware and firewalls; Best estimate would be about $100k of equipment	Yes	No
Second Factor Authentication Tools	Configuration and maintenance; .5 hours per employee access to the system	Yes	No
Audit Trail tools	Build in a write audit data and controlled access to the data; $10,000 to buy a solution	Yes	No
Central Event Log Tools	$5,000 startup costs; $2,000/year to maintain	Yes	No
Reviewing Event Logs Daily	.5 hours per day	Yes	No
Create Incident Response Plan(s)	4 hours per year	Yes	Yes
Create Incident Response Tests	3 hours per year	Yes	Yes
Intrusion Detection Technology	Depends on the solution, could be included in annual firewall costs, $15,000/year	Yes	No

Table 1. Example of PCI Costs for 10 employees + 3 External Web Applications + 2 Internal Web Applications

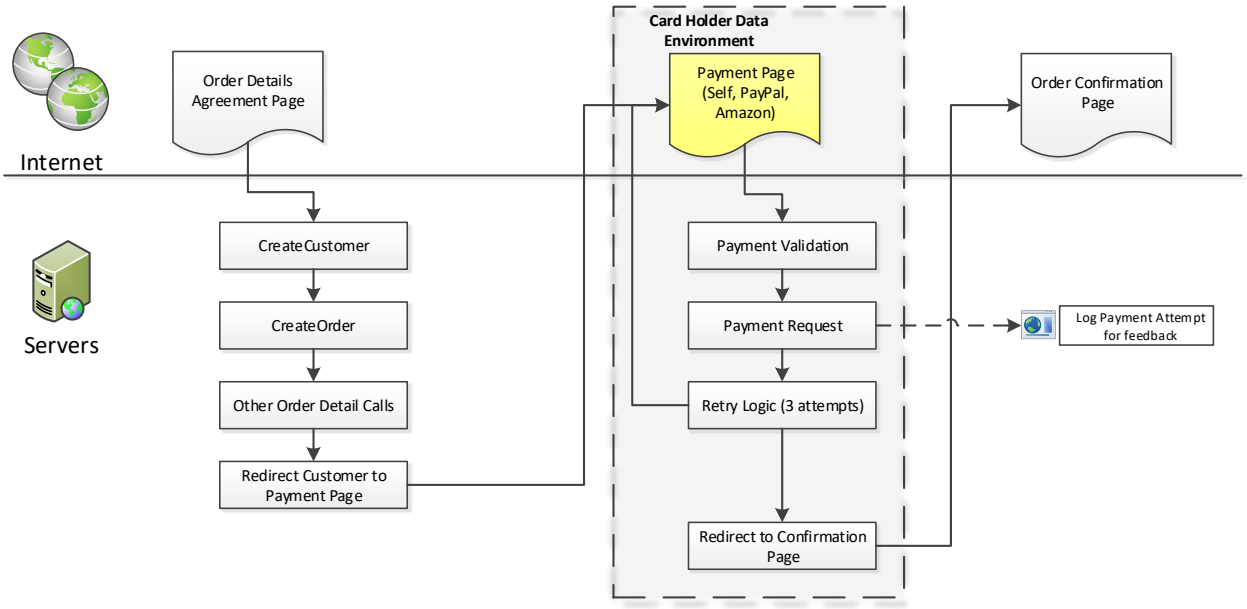
One way to solve this is to work through the process and develop the needed policies and technologies to become PCI Level X compliant. Another solution is to outsource the credit card data and hosting to a PCI-compliant vendor. When outsourcing, keeping the branded feel of the application is key, along with a solution that will work seamless between the company and the vendors' while maintaining a PCI-compliant process.

High-Level Solution

Most people have heard of PayPal or Amazon Express to accept a credit card transaction and have potentially seen how the solution pops-up a window to accept the credit card transaction and then return the customer back to the company's order process, but each of those solution takes the user to a

PayPal- or Amazon-branded solution potentially distracting the user from your brand. On the flip side of this, the customer may be more in tuned to using this solution because their credit card details are stored in only one place but for you, the merchant, the cost of accepting the payment from these sources may be higher than you can negotiate with a merchant services provider or working directly with a credit card processor like Paymentech or TSYS.

Another solution is to use a branded-page hosted by an external PCI-compliant vendor. In this solution, the customer does not "leave" your systems but are taken through the process without interruptions. The solution would communicate the pass over between the servers behind the scenes and provide the necessary interfaces for customer service to find transactions or assist the customer during the transaction.



Solution Examples

BFC has worked with a number of companies to provide a branded solution to move the card holder data environment outside of the company's network to reduce the overall scope of the PCI compliance audit. In our first instance of this type of solution, BFC worked with DHL provide the credit card entry form for the DHL WebShip application. The DHL WebShip application would take the shipment details from with the DHL environment and when they were ready to show the credit card form, the servers would take and then the credit card entry form would be presented to the user for payment.

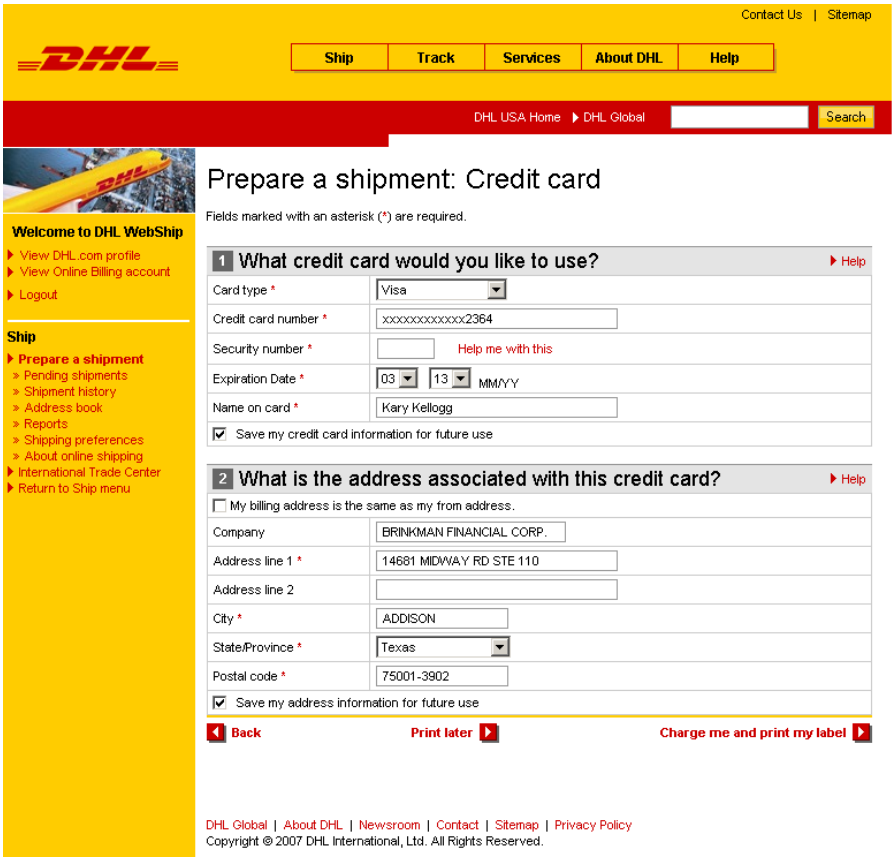


Figure 2. BFC Hosted Credit Card Entry Page (circa 2011)

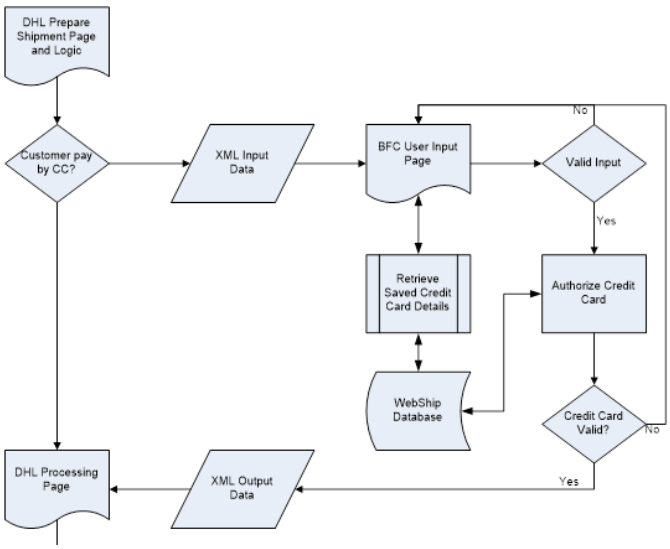


Figure 3. Original Payment Flow

Once the payment details were made, the transaction would be processed. Over the course of the hosting the solution, DHL had made three different processor changes and saw no design changes within the application due to the nature of our Gateway being able to accept a different processor when desired.

With DHL, PCI was just becoming a standard that all companies needed to follow. In this instance, creating the network segmentation and training a large staff would require a large amount of time. By outsourcing the solution, they were able to be PCI compliant and keep their data secure over the course of the solution.

In another example, we worked with World Ventures to provide a branded-solution to capture a credit card and submit the credit card details into their processor in order to return a token back to their application for future recurring or shopping charges. This allowed World Ventures to continue to collect card holder data without having to maintain the data in their networks. World Ventures utilized two different branded pages and they appeared to the end user as the same company even if the URL changed as they navigated.

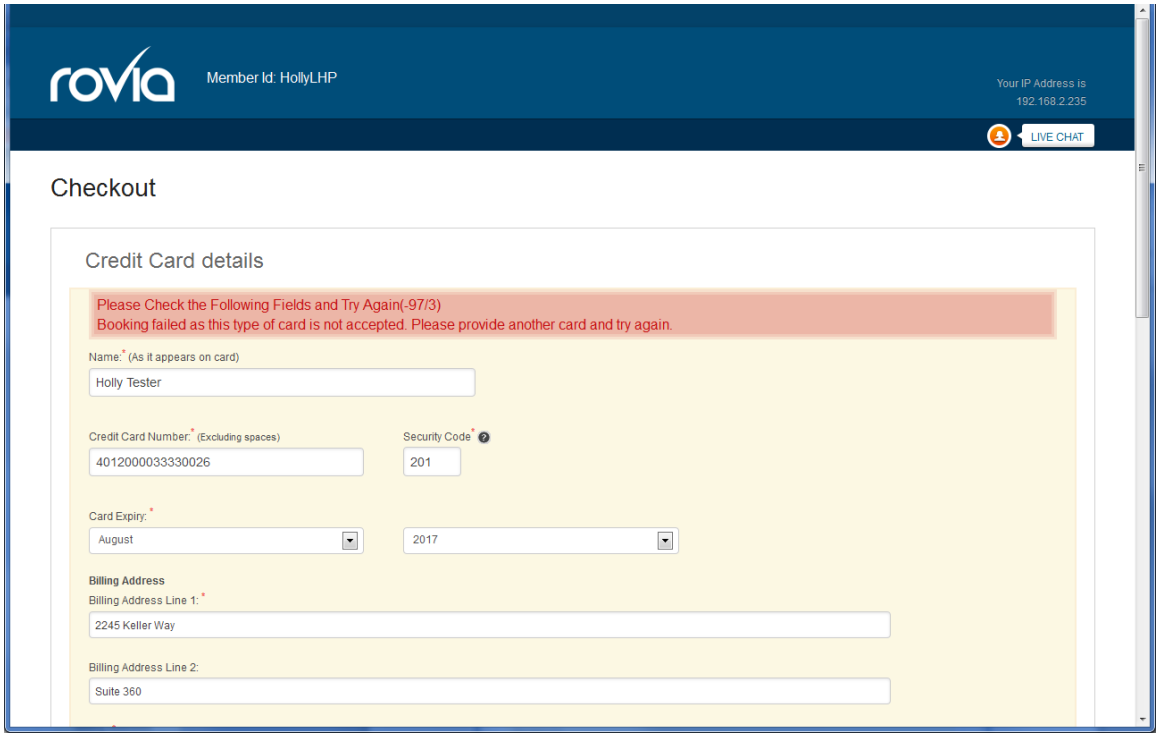


Figure 4. World Venture's Rovia-Branded Credit Card Entry Form (circa 2014)

Business Benefits

Regardless of the solution, working with a partner that is attentive to your needs helps you keep your business working smoothly and without the headaches of trying to solve problems created by that partner. With Brinkman Financial Company, we have worked with companies that are just entering the PCI space or even those just needing some additional fact-finding and education for how the credit card processing network works.

Sometimes it is just easy to add a small branch from a process flow rather than having to redesign a lot of things to accomplish the same thing you are doing today.

Summary

With BFC's solutions, your company can continue to accept and/or handle credit cards with a branded solution that can integrate into your environment all without having to re-invent the wheel and update all your internal processes to become PCI compliant. We'd love to hear the challenges you are experiencing to help solve when dealing with payment processing – phone 972-242-8090 x 2 or email us at sales@bfc-usa.com.