TECHNICAL ASSESSMENT
WHITE PAPER

Coalfire
IT Audit and Compliance

PCI Compliance in Multi-Site Retail Environments

Executive Summary

As an independent auditor, Coalfire seeks to be a trusted advisor to our clients. Our role is to help them understand information technology risks, the applicable compliance requirements and their many options for controls that can be deployed to manage those risks. We then guide them in making the right decisions – all things considered – for their businesses, balancing risk, cost and control effectiveness.

We work with dozens of multi-site merchants in many industries, and most of these merchants must maintain compliance with the Payment Card Industry Data Security Standard (PCI DSS) in stores that are widely distributed. Typically, we see strong controls in the data center and back office/headquarters. As auditors, we also test their entire operation and are required to do field work (control testing) at store locations. In that work, we often hear – and discover – that deploying and maintaining cost-efficient and effective controls in a multi-store store environment is the leading obstacle to attesting to PCI DSS compliance.

This white paper outlines a controls approach that Coalfire has observed, tested and found to be PCI-compliant for multiple, multi-site retailers. In addition, we offer some lessons learned from the forensics investigations at compromised merchants, where we have also seen the results of inadequate controls and non-compliance.

Prepared For:

RELIANT SECURITY

Rick Dakin, QSA
President & Chief Security Strategist

Karl Steinkamp, QSA, CISSP, CISA, NSA-IAM
Senior Security Auditor

Table of Contents

The Business Challenge

The data breach problem for card processing continues to grow and the resulting identity theft has become a matter of public record. There have been many high-profile breaches involving national apparel and home goods retailers, grocery chains, and specialty retailers. The past four years have revealed an escalating series of consumer credit card information breaches.

Faced with mounting liability, rapidly escalating damage to consumers, and erosion of customer confidence in electronic payment systems, the Payment Card Industry (PCI) developed a Data Security Standard (DSS) for businesses that store, process and transmit credit card data.

Since 2005, compliance requirements have been increasingly enforced and critical failures in maintaining compliance with the PCI DSS have resulted in significant penalties for both the processors and the merchants. Compliance with the PCI security standards are no longer optional for merchants. However, many merchants have found achieving compliance with the PCI DSS in a multi-site retail environment to be complex and expensive.

In the early stages of PCI DSS enforcement, the hackers were stealing databases that contained cardholder data. The primary target of attack was a server in the corporate data center or in the back office for a large retail location. The deployment of sophisticated security programs at these locations where large stores of cardholder data were vulnerable resulted in a shift in tactics by the hacking community. Today, the primary targets are small retail locations where as few as 500 stolen credit cards can net the cyber criminals with a $100,000 payback.

This shift in threat has not been fully addressed by the retail community, and specifically not by retailers with distributed store operations. The focus of attack is now the store location or a specific POS platform while the focus for the security program remains, in large part, the back office data center. Until retailers shift their focus to improving retail location security, the number of data breaches will continue and the losses due to cardholder compromise will continue to mount. The business case for improving retail store security is much more compelling today than in previous years.

In addition, many merchants are not as secure as they think. We have worked with clients whose previous auditor found them to be compliant and issued a 'green' Report on Compliance. They are often surprised when we discover compliance gaps in their distributed store locations. As their advisory, we seek to educate them on the business risks and control options.

Distributed Store Security Requirements

Retail IT departments are charged with doing more with less staff, and PCI can be viewed as a drain on resources. This is especially true in early compliance efforts, where store environments required a "mini-data center" approach involving multiple security devices and customized configurations. These security devices can be expensive to deploy and difficult to manage in a multi-site retail environment. Store personnel seldom have the skills or capacity to manage such devices and ensure ongoing compliance.

These controls solutions required large up-front capital and deployment expenditures and had high "total cost of ownership" due to ongoing maintenance and operation of the solution. Finally, they had reliability issues, which threatened their ability to perform credit card transactions. Many retailers can't afford the time required to work out compatibility and configuration issues normally associated with custom systems integration efforts.

Although many companies have taken steps toward meeting PCI requirements, two recent studies from the Ponemon Institute[1] and InsightExpress[2] indicate that significant compliance gaps remain. The card associations and acquirers have tried a variety of fines and incentives to encourage compliance across the merchant population. However, adoption of PCI, particularly at the store systems level, remains a significant challenge.

For all of its security drawbacks, the retail environment often has two advantages in achieving PCI compliance:

- Most store systems environments are virtually identical across retail chains, so investment to produce a cost-effective solution in one store can be leveraged across all of them. Additionally, data security controls and processes can be more easily automated across multiple homogeneous environments.
- Proprietary, high-performance hardware and software is generally not required based on the generally low volume of transactions per store. The environment is ideally suited for standardized COTS[3] components and for virtualization. This can allow a single appliance to perform many security functions at once – reliably and predictably.

1. CSO Magazine, "RSA 2010: Why 41 Percent of You Would Fail a PCI Audit," March 1, 2010
2. InsightExpress Whitepaper, "Organizations See PCI as a Benefit t, Not a Burden," January 2011
3. Commercial off -the-shelf (COTS) is a term for software or hardware, generally technology or computer products, that are ready-made and available for sale, lease, or license to the general public.

An "all-in-one" Approach to Low Cost Store Security

The traditional data center-oriented security solutions may not be the most cost-effective in remote store locations. Coalfire has seen several early solutions that vary from a totally outsourced service to a self-contained "single box" security appliance that can reduce both the capital costs to achieve compliance as well as sustain security services.

One security appliance that Coalfire has audited at several large retailers is the Redbox solution provided by Reliant Security. In order to reduce costs, Reliant Security added multiple features to the Redbox that contains software and hardware components and operates as a Virtualized Security Appliance that resides in stores. The security applications were designed to meet PCI DSS standards across the 12-control objectives specified in the PCI DSS. Coalfire assessed the Redbox solution to ensure its PCI DSS compliance.

Assessment Results – MPS Redbox: a PCI-Compliant Solution

Coalfire is a Qualified Security Assessor Company (QSAC) that provides both merchant assessments under the PCI audit procedures and payment application validations.

In 2008, Coalfire completed an audit of a PCI Level 1 merchant, which included a full evaluation of the Redbox architecture and field testing of the deployed controls across multiple store environments. The resulting Report on Compliance (ROC) validated the full suite of Redbox controls. In fact, the easiest part of the testing for the cardholder environment was the store-level controls managed by the Reliant Redbox. In November 2010, we evaluated a PCI Level 1, 1,200-store retail implementation of the Redbox and issued a fully validated Report on Compliance (ROC). The solution functioned effectively and simplified the process of demonstrating compliance with the PCI DSS. A summary of the embedded controls is provided in the Appendix of this white paper.

Based on these and other client projects, Coalfire believes the Reliant Redbox meets a variety of PCI control requirements and reduces risk to cardholder data in multi-site retail environments. In addition, our clients have reported that the Redbox has helped them lower the cost for achieving and maintaining PCI.

About Coalfire

Coalfire is a leading assessor in the payment card industry validating PCI compliance across the largest service providers and merchants throughout the U.S. and Canada. Coalfire conducts over 1,000 assessments each year, and is actively engaged with many leading retailers, technology vendors and service providers. For more information, visit www.coalfiresystems.com.

****

Copyright © 2011 Coalfire Systems, Inc. All rights reserved.

Appendix

As reference, we have included this Appendix, containing a requirement-by-requirement analysis of the Redbox-provided controls that we expect to see in a deployed environment. Note: These requirements must always be validated with appropriate field testing by a QSAC.

Requirement	Result	Specific Findings
1. Install and maintain a firewall configuration to protect cardholder data.	✔	• Redbox systems include a built-in stateful inspection firewall. • Redbox systems maintain built-in controls to secure and synchronize router configurations to ensure that the running and current configurations are adequately maintained. • Redbox firewall controls what ports and services are allowed to communicate between firewall-controlled segments, as well as, allowing for flexibility of the end Client needs to specific ports and services for business and cardholder processing. • Redbox firewall controls implement network address translation (NAT) to prevent IP spoofing and masquerading attacks from affecting the organization's cardholder data environment.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.	✔	• Redbox systems maintain strict control of configuration management of the individual Redbox instances, as well as, connected systems. • Redbox maintain controls to ensure that default, insecure, and unnecessary ports and services are disabled on Redbox and connected systems. • Non-console administrative access and management of systems is only conducted over encrypted and secured ports and services, to include HTTPS and SSH, with strong encryption algorithms and ciphers utilized.
4. Encrypt transmission of cardholder data across open, public networks.	✔	• Remote management and access to systems over public networks is conducted using only secure communications within a VPN tunnel.
6. Develop and maintain secure systems and applications.	✔	• Redbox technologies have implemented patch management processes to ensure that the Redbox and all connected systems within the environment maintain current security and operating system patches every 30 days.
8. Assign a unique ID to each person with computer access.	✔	• Redbox implements processes and technologies for user management to ensure that all users within the cardholder environment are unique to a user for individual accountability. • The Redbox architecture implements strong two factor authentication through the use of the latest PhoneFactor application. The infrastructure supports stand alone and Active Directory integrated environments. • Strong password management is supported and enforce by Redbox security controls and architecture.
10. Track and monitor all access to network resources and cardholder data.	✔	• The Redbox architecture maintains a built-in centralized log management system for collection, analysis, and alerting for all cardholder systems and devices. Logs and retention are secured and retained to PCI log retention specifications. • The Redbox architecture allows for Network time Synchronization (NTP) management and propagation. • File integrity for critical log files (applications, operating systems, etc) is conducted through the built-in file integrity management checks. All files are hashed and a daily MD5 integrity check is conducted to validate file changes.
11. Regularly test security systems and processes.	✔	• The Redbox system facilitates quarterly wireless analyzer scanning through the built-in wireless intrusion detection management console and wireless drone. Wireless detection is enabled and continually monitors the retail environment for the presence of wireless networks. Through the Redbox management interface, management can efficiently review and audit the presence of wireless networks. • The Redbox system facilitates quarterly internal vulnerability scanning of all devices through a built-in and internal Nessus scanner instance. Scans are conducted and reports populated to a centralized portal for management review and retention. • Each Redbox maintains an external Snort IDS sensor to continually identify the presence of suspicious and/or malicious network communications to the cardholder environment. Updates are continually conducted to ensure that current signatures are maintained.