AuthAnvil
Password Solutions

# AuthAnvil for Retail IT

*Exploring how AuthAnvil helps to reach compliance objectives*

scorpion software | A Kaseya Company

# AuthAnvil for Retail IT

## Exploring how AuthAnvil helps to reach compliance objectives

## Whitepaper

As companies extend their online business processes to encompass the acceptance of credit card payments, they need to ensure that they meet compliance objectives being set forth by major credit card companies. The *Payment Card Industry Data Security Standard* (PCI DSS) was created as a guideline to help organizations that process card payments prevent credit card fraud, hacking and various other security issues. In this paper, we will explore the guidance of the PCI standard and demonstrate how AuthAnvil can help to reach compliance objectives.

scorpion software | A Kaseya Company

**Copyright © 2013, Scorpion Software Corp.**
**All Rights Reserved**

## Table of Contents

Introduction ..... 3
PCI DSS 101 ..... 3
The PCI DSS Framework ..... 3
What Merchant Level is your business categorized as? ..... 4
Why is it important for your business to comply? ..... 4
What are the consequences if you don't comply? ..... 4
How does AuthAnvil help meet PCI requirements? ..... 5
Strong Access Control Measures ..... 5
PCI DSS Requirement 8.2 ..... 5
PCI DSS Requirement 8.3 ..... 5
PCI DSS Requirement 8.4 ..... 6
PCI DSS Requirement 8.5 ..... 6
Auditing and Monitoring ..... 7
PCI DSS Requirement 10.1 ..... 7
PCI DSS Requirement 10.2 ..... 7
PCI DSS Requirement 10.3 ..... 7
PCI DSS Requirement 10.5 ..... 7
PCI DSS Requirement 10.7 ..... 8
Conclusion ..... 8
About Scorpion Software ..... 8

# Introduction

As companies extend their online business processes to encompass the acceptance of credit card payments, they need to ensure that they meet compliance objectives being set forth by major credit card companies. The *Payment Card Industry Data Security Standard* (PCI DSS) was created as a guideline to help organizations that process card payments prevent credit card fraud, hacking and various other security issues.

Understanding what PCI DSS is and how it may affect your own business helps to demonstrate why strong two-factor authentication systems like AuthAnvil are vital to protect your organization.

# PCI DSS 101

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. It was developed by the *PCI Security Standards Council*, which was founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International. More information about the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection can be found at www.pcisecuritystandards.org. You can find the actual PCI DSS specifications at: https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf.

## The PCI DSS Framework

PCI DSS represents a common set of security due diligence practices that help ensure the safe handling of payment card data. This standard comprises 12 distinct requirements that are designed to meet compliance objectives through the PCI DSS Framework, broken down as follows:

**Category 1. Build and maintain a secure network**
- Requirement 1: Install and maintain a firewall configuration to protect cardholder data.
- Requirement 2: Do not use vendor supplied defaults of system passwords and other security parameters

**Category 2. Protect (cardholder) data in transit or at rest**
- Requirement 3: Protect stored cardholder data
- Requirement 4: Encrypt transmission of cardholder data across open, public networks.

**Category 3. Maintain a vulnerability management program**
- Requirement 5: Use and regularly update anti-virus software or programs
- Requirement 6: Develop and maintain secure systems and applications

**Category 4. Implement strong access control measures**
- Requirement 7: Restrict access to cardholder data by business need-to-know.
- Requirement 8: Assign a unique ID to each person with computer access
- Requirement 9: Restrict physical access to cardholder data

**Category 5. Regularly monitor and test your IT infrastructure**
- Requirement 10: Track and monitor all access to network resources and cardholder data
- Requirement 11: Regularly test security systems and processes

**Category 6. Maintain an information security policy.**
- Requirement 12: Maintain a policy that addresses information security for employees and contractors.

Compliance of these requirements can be summarized into three (3) main stages:

1. **Event collection**
   Secure collection and storage of all event data so that it is available for review and analysis.
2. **Reporting**
   Provide evidence that safeguards are in place to protect data and prove compliance as required if audited.
3. **Monitoring**
   Have systems in place to monitor access and usage of sensitive data, and alert administrators of problems immediately to allow for fast remediation in the face of failure.

## What Merchant Level is your business categorized as?

Businesses that process credit cards are defined as "Merchants" within PCI DSS. A merchant is categorized according to the number of transactions that they process within a twelve month period:

- Level 1: Merchants with more than 6 million card transactions & merchants which cardholder data has been compromised.
- Level 2: Merchants with card transactions between 1 and 6 million
- Level 3: Merchants with card transaction between 20,000 and 1 million
- Level 4: All other merchants

These levels determine the validation processes that a merchant must undertake in order to achieve and maintain compliance.

Meeting PCI DSS compliance calls for merchants to demonstrate that they have fulfilled their obligations in accordance with all twelve requirements. For Level 1 merchants, they are required to have an annual on site security audit performed by a Qualified Security Assessor (QSA) and complete quarterly network scans with an Approved Scan Vendor (ASV). All other merchant levels are required to fill out an annual self assessment questionnaire and complete a quarterly network scan with an ASV.

## Why is it important for your business to comply?

There is a lot of confusion on who is required to meet the compliance objectives of PCI DSS. Some businesses believe it is only for larger US companies, not realizing that PCI DSS is a global standard for ANY business that accepts and stores credit card payment information. Typically Service Providers (the agents that process cards on behalf of the merchant) are responsible for working with the merchants and ensuring that they are adequately protected. Most Service Providers will simply NOT allow you to accept credit card transactions if you do not comply with their requirements. It therefore becomes critical to comply with PCI DSS if you wish to complete credit card orders through a Service Provider, and collect the revenues from the transaction.

## What are the consequences if you don't comply?

If credit card data is compromised, fines of up to $500,000 can be levied from the major credit card company affected to the Service Provider. In turn, these providers usually contractually oblige merchants to indemnify and reimburse them for such fines, and usually immediately block all future credit card transactions from occurring until the compromised merchant meets the requirements for Level 1 Merchant obligations.

For many businesses, this may prove to be too costly and will cause business closure. For those who can carry on after such a breach, the new stringent requirements typically shackle the business in its online ordering process, significantly limiting the ability to collect revenues from credit card transactions. This is further compounded with secondary consequences such as further business interruption, bad publicity and possible legal actions from customers affected.

## How does AuthAnvil help meet PCI requirements?

Requirement 8.3 of PCI DSS specifically identifies the requirements to "*implement two-factor authentication for remote access to the network by employees, administrators and third parties.*". As a two-factor authentication solution for the protection of Windows and Unix platforms, AuthAnvil meets this objective and provides the expected technical safeguards as required to satisfy PCI DSS requirements. Furthermore, AuthAnvil's secure design and defaults meets compliance objectives in many of the other requirements as set forth by the PCI standard.

The remainder of this paper will identify the applicable requirement sections that AuthAnvil can satisfy, and demonstrate how AuthAnvil meets these compliance objectives with its use.

## Strong Access Control Measures

Under Category 4 of PCI DSS, merchants are required to *Implement Strong Access Control Measures*. The use of AuthAnvil helps our customers ensure that users accessing systems with sensitive credit card information are who they claim to be. Requirement 8 requires merchants to *Assign a unique ID to each person with computer access*, and is further broken down into following subsections:

### PCI DSS Requirement 8.2

> ***Requirement 8.2:*** *In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: 1) Password 2) Token devices (e.g., SecurID, certificates, or public key) 3) Biometrics*

AuthAnvil exceeds this requirement with the combination of a 4 to 8 digit personal user PIN and the use of a hardware authentication token that randomly generates a new 8 alphanumeric one time password (OTP) with each use. Combined together, this unique single use 12 to 16 character *passcode* offers strong authentication that cannot be forged.

### PCI DSS Requirement 8.3

> ***Requirement 8.3:*** *Implement two-factor authentication for remote access to the network by employees, administrators, and third parties.*

AuthAnvil enables organizations to meet this requirement by deploying two-factor authentication within their network and can act as a gatekeeper to provide authentication services to all incoming untrusted remote connections. Included in this are facilities to:

- Provide strong authentication to incoming VPN and firewall users through the *AuthAnvil RADIUS Agent*, an extension built on top of Microsoft's Internet Authentication Service.

- Provide strong authentication to incoming terminal services and RDP users through the *AuthAnvil Windows Logon Agent*, a Windows Logon replacement built to intercept logon requests to Windows servers and workstations.
- Provide strong authentication to Line of Business (LOB) web applications through the *AuthAnvil TokenValidator Web Service*, a standards-based SOAP/XML web service that allows web applications to consume AuthAnvil authentication services.
- Provide strong authentication to Line of Business (LOB) standalone applications through the *AuthAnvil DCOM Bridge*, a distributed COM architecture that allows applications vendors to call AuthAnvil authentication services without any knowledge of web services.
- Provide strong authentication to Microsoft's Small Business Server (SBS) 2003 through *RWW-Guard*, a logon replacement agent for Remote Web Workplace.

Further to this, *Authorized AuthAnvil Partners* offer implementation and integration services which allow AuthAnvil customers to quickly deploy two-factor authentication and makes it simple for businesses to strongly authenticate users accessing sensitive resources via remote connections.

## PCI DSS Requirement 8.4

> ***Requirement 8.4:*** *Encrypt all passwords during transmission and storage on all system components*

AuthAnvil stores all related authentication key information about its tokens and PINs in an encrypted fashion when at rest on disk within SQL server. AuthAnvil uses the standards-based AES algorithm to encrypt all such information and further protects the encryption keys by storing them securely in the DPAPI store of the Windows server where AuthAnvil resides.

When transmitting the user's PIN and OTP between remote agents and the AuthAnvil server, communications are secured with the use of 128bit encryption within a SSL stream. This is further protected with the use of IP based access control lists (ACL) to deny communications between untrusted remote hosts and the AuthAnvil server.

## PCI DSS Requirement 8.5

> ***Requirement 8.5:*** *Ensure proper user authentication and password management for non-consumer users and administrators on all system components*

AuthAnvil meets this requirement by forcing remote users to reliably prove their identity through the use of their authentication token prior to access being granted to the sensitive system(s) being protected.

## Auditing and Monitoring

Under Category 5 of PCI DSS, merchants are required to *Regularly monitor and test [their] IT infrastructure.* The reporting facilities within AuthAnvil helps our customers to provide oversight into the use and access to sensitive systems and helps to verify that users and administrators accessing these systems are complying with established security policies as required in PCI DSS. Requirement 10 requires merchants to *Track and monitor all access to network resources and cardholder data*, and is further broken down into following subsections:

### PCI DSS Requirement 10.1

> ***Requirement 10.1:*** *Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*

AuthAnvil provides detailed audit logs of all authentication requests and matches each request to the individual user. Even when authenticating to administrative accounts such as *Administrator* or *root*, AuthAnvil records and reports the actual user that logged in with administrative privileges by associating their token to the transaction.

### PCI DSS Requirement 10.2

> ***Requirement 10.2:*** *Implement automated audit trails for all system components to reconstruct key events*

AuthAnvil provides detailed reporting on all completed authentication requests and provides an audit history of all system level objects that are added, modified and/or deleted. All administrative activities to the AuthAnvil configuration is recorded and timestamped to allow for easy reconstruction of key event timelines as required by information security best practices.

### PCI DSS Requirement 10.3

> ***Requirement 10.3:*** *Record audit trail entries*

AuthAnvil records all audit logs to a SQL database, and provides easy analysis and review through SQL queries and views.

### PCI DSS Requirement 10.5

> ***Requirement 10.5****: Secure audit trails so they cannot be altered*

AuthAnvil protects its audit log tables with standard SQL access controls with mixed mode authentication and a restricted user account. If required, *Authorized AuthAnvil Partners* with experience with SQL Server deployment can isolate the system and provide stronger access control and role separation to further protect the audit logs and ensure that they cannot be altered through the use of SQL mirroring and replication.

### PCI DSS Requirement 10.7

> ***Requirement 10.7:*** *Retain an audit trail history for at least one year, with a minimum of three months online availability*

Through the use of the *AuthAnvil Backup and Restore* tools, it is possible for customers to backup and restore various audit history data sets for analysis for any period required by auditors. By default AuthAnvil does not truncate or clear logs, and provides no facility to do so to prevent the unintentional (or intentional) destruction of audit history data.

## Conclusion

For organizations that carry out business transactions involving the use of credit cards, meeting the compliance objectives of PCI DSS is highly important to reduce the risk of business interruption and the costly financial burden that may be placed on those who fail to comply. Fines, bad publicity and possible legal actions can be detrimental to the growth of your business on top of the business interruption that is sure to occur in the face of a breach in the safeguarding of sensitive credit card data.

Implementing strong two-factor authentication to provide the technical safeguards as required in PCI DSS is important to your business, and will go a long way towards helping you achieve compliance. Scorpion Software's AuthAnvil Strong Authentication System can help reduce the risk of such business threats and provide assurance levels that only *identified* and *authorized* personnel gain access to such sensitive information.

## Ready to learn more?

Our no-obligation authentication automation assessment evaluates your current password management and access control programs for areas of improvement. From there we can offer recommendations and guidance that will have an immediate impact on your business.

## About Scorpion Software

Scorpion Software Corp provides the premium solution for SMBs to reduce the risks associated with the use of weak static reusable passwords and provide a higher level of confidence that only authorized users can access their company's most important business assets - their proprietary information. Headquartered in British Columbia, Canada, Scorpion Software helps small businesses manage online risk while offering unprecedented password protection. More information about the company is available at www.scorpionsoft.com.

What Does AuthAnvil Cost?

Password security shouldn't be expensive. AuthAnvil offers a full-featured password management system at a cost similar to the more limited password management systems of some of our competitors.

Click here to get a pricing quote