



Meeting the PCI Security Standard

A Solidcore White Paper





Meeting the PCI Data Security Standard

A Solidcore White Paper

Solidcore Systems, Inc. delivers innovative software solutions that facilitate an enterprise's ability to gain cost-effective and categorical control of its IT infrastructure and realize immediate and tangible value across areas of change control, compliance, and security. These benefits enable retailers and other credit card processing entities to significantly reduce the cost of complying with the PCI Data Security Standard. This Solidcore white paper describes the PCI Data Security Standard and provides an explanation of how the Solidcore solution can be leveraged to comply with its requirements.



Overview

Identity theft and credit card fraud is a large and growing problem. The Federal Trade Commission estimates that almost 10 million consumers were affected last year, at a cost of close to \$50 billion. In order to combat this growing menace, Visa, MasterCard, American Express, Diners Club, Discover and other major credit card providers joined together to introduce a compliance standard - the payment Card Industry (PCI) Data Security Standard. The standard unites and supersedes the individual compliance standards such as Visa's CISP and MasterCard's SDP standards that were in place prior to the introduction of PCI. This program is intended to protect cardholder data wherever it resides, ensuring that members, merchants and service providers maintain the highest levels of information security. The PCI standard came into effect on December 14th, 2004, and **merchants and service providers are required to be PCI compliant by June 30th, 2005.**

Like all compliance programs, PCI consists of two separate components, both of which must be implemented in order to be PCI compliant:

1. Compliance with PCI requirements
2. Validation of PCI compliance

Each of these components is discussed in more detail below.

PCI Requirements

PCI mandates that all merchants follow twelve requirements, listed below. In addition, there is an implicit thirteenth requirement to verify compliance with PCI – often overlooked but an integral part of any PCI compliance program.

PCI Requirements	
1	Install and maintain a firewall configuration to protect data
2	Do not use vendor-supplied defaults for passwords and 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 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.
PCI Compliance	
13	<i>Verify PCI compliance</i>

The requirement to verify PCI compliance is discussed in more detail in the next section.

PCI Compliance

The first thing to note about PCI compliance is that the cost of non-compliance is high. In the event of a security breach, merchants must immediately investigate the incident and limit the exposure of cardholder data, must immediately notify the appropriate credit card entity and report on its investigation of the incident. Merchants or service providers that have been compromised but found to be PCI compliant at the time of the security breach will not be fined. **However, any merchant or service provider that is compromised and not PCI compliant at the time of the breach, is subject to fines - up to \$500,000 per incident.**



Credit card issuers divide its merchants into four levels based on the number of transactions processed every year, as shown in the table below.

Merchant Level	No. of transactions(annual)
Level 1	> 6 million
Level 2	150,000 – 6 million
Level 3	20,000 – 150,000
Level 4	< 20,000

Each level is subject to a different set of compliance activities, with the strictest rules applied to level 1 merchants. In addition to transaction volume, any merchant that suffered a hack or an attack that resulted in account data compromise will automatically be required to meet level 1 compliance requirements. Further, the card issuer may, at their discretion, require any merchant in its network to meet level 1 requirements. In view of this, our recommended best practice is to follow level 1 requirements regardless of activity level. This white paper will focus on the compliance validation activities required of level 1 merchants.

Participating merchants must pay for their own PCI compliance assessment, and the cost of compliance depends on the extent to which they are already in compliance. A level 1 merchant needs to submit an annual **Report on**

Compliance, validated by an approved independent auditor, or by an internal audit department, provided that a letter signed by an executive-level officer of the company accompanies the report.

For level 1 merchants required to undergo an annual compliance review, the scope of validation is focused on systems or system components related to authorization and settlement where cardholder data is processed, stored, or transmitted.

The Solidcore Solution

Solidcore provides categorical control over IT infrastructure, enabling retailers and other merchants to fulfill PCI requirements and validate PCI compliance in an efficient and cost-effective manner.

Of the twelve PCI requirements, Solidcore’s primary benefit covers one of the most operationally costly requirements (requirement 10), and provides significant additional benefit for another six requirements (requirements 3, 5, 6, 7, 11 and 12). The remaining requirements are either “best practice” requirements or network requirements not addressed by Solidcore.

PCI Requirement	Solidcore
1 Install and maintain a firewall configuration to protect data	Network
2 Do not use vendor-supplied defaults for passwords and security parameters.	Best Practice
3 Protect stored data	✓
4 Encrypt transmission of cardholder data and sensitive information across public networks	Network
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 unique ID to each person with computer access	Best Practice
9 Restrict physical access to cardholder data	Best Practice
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.	✓
PCI Compliance	
13 <i>Verify PCI compliance</i>	☑



Most importantly, in addition to helping with PCI requirements, Solidcore greatly simplifies the PCI compliance verification process (the implicit “thirteenth requirement”), a benefit not addressed by other PCI solutions.

The remainder of this section will focus on how Solidcore can help with these requirements.

Benefits

- **Protect stored data**

Solidcore provides protection against unauthorized access to cardholder data by ensuring that any unauthorized code that tries to access cardholder information will be blocked from doing so. In addition, Solidcore can ensure that protected data (such as cardholder information) cannot be modified outside of an authorized change process. Any attempts to do so will be prevented, and an alert will be generated to enable further investigation.

- **Use and regularly update anti-virus software**

Compliance requires continuous virus scanning and real-time signature updates, an operationally cost-prohibitive demand on most production systems. Continuous anti-virus protection is very CPU intensive and real-time signature updates require IP connectivity to the internet, which is not always possible or prudent. Signature distribution mechanisms can be operationally expensive and suffer from the same drawbacks as patch deployment systems. The tension between complying with the PCI requirement and lowering operational cost is completely removed with Solidcore. The Solidcore solution prevents unauthorized programs from running on deployed systems, period. This categorical control ensures that zero-day viruses, worms, trojans and other malicious programs cannot compromise cardholder data security. Anti-virus systems may still be run as an added precaution, but scan frequency can be significantly reduced, and signature updates can be “batched” rather than real-time.

- **Develop and maintain secure systems and applications**

The PCI standard requires that security patches be installed within 30 days of release. This requirement, as with all security update requirements, highlights a conflict between a need for timely updates of patches to keep systems secure and a need to adequately test patches before deployment. With Solidcore technology, it is no longer necessary to manage the conflicting demands of adequately testing new security updates while also deploying patches in a timely manner. The Solidcore solution prevents unauthorized programs from running on deployed systems, period. As mentioned earlier, this categorical control ensures that viruses, worms, trojans and other malicious programs cannot compromise cardholder data security.

- **Restrict access to data by business “need to know”**

Most solutions that attempt to enforce the separation of roles on a “need to know” basis suffer from a critical drawback: to give access an organization loosens control. **However**, the Solidcore solution ensures that no unauthorized changes can be made on deployed systems, even with administrator privileges. Solidcore implements local access lockdown, restricting the ability of local administrators of computers to effect changes, and a dual key control mechanism for changes to deployed systems, eliminating the risk of unauthorized or unintended change. Every change activity is logged to provide a full audit trail for compliance and remediation. These changes are linked with an organization’s change control system to provide a one-to-one mapping showing only approved changes are made.

- **Track and monitor all access to network resources and cardholder data**

The PCI standard states: “logging mechanisms and the ability to track user activities are critical.” It goes on to define requirements around maintaining secure audit trails and using file integrity/change detection mechanisms. The Solidcore core solution allows an organization to prevent and alert rather than detect and remediate. Solidcore tracks all



change events in real-time and can generate alerts or simply aggregate the information for reporting. Solidcore can also integrate with change approval systems so that the reconciliation between the set of approved changes and the set of actually deployed changes is an automated, closed-loop process. More than tracking changes, however, Solidcore can also prevent unauthorized changes – discussed in more detail below.

- **Regularly test security systems and processes**

Solidcore provides the ability to define and, most importantly, *enforce* change processes throughout the enterprise. Solidcore ensures that changes that violate the corporate change control process cannot occur. Solidcore provides complete audit trails of all attempted unauthorized actions. These events can be integrated into other enterprise monitoring and testing tools for further analysis. Further, because of the local access lockdown feature discussed earlier, audit trails are not under local administrative control, ensuring that they cannot be tampered with. Solidcore tracks all changes to critical systems to validate that unauthorized changes that violate corporate processes did not occur.

Using Solidcore to verify PCI Compliance

The PCI Data Security Standard lays out a set of twelve requirements, as well as an implicit thirteenth requirement (verifying that the first twelve requirements have been followed). Solidcore is a proactive solution to the PCI standard. Solidcore’s deploy-and-forget solution provides coverage for one of the most operationally costly requirements, and provides significant benefit for six other requirements. In addition, Solidcore greatly simplifies the process of demonstrating PCI compliance to internal and external auditors.

Summary

The PCI Data Security Standard lays out a set of twelve requirements, as well as an implicit thirteenth requirement (verifying that the first twelve requirements have been followed). Solidcore is a proactive solution to the PCI standard. Solidcore’s deploy-and-forget solution provides coverage for one of the most operationally costly requirements, and provides significant benefit for six other requirements. In addition, Solidcore greatly simplifies the process of demonstrating PCI compliance to internal and external auditors.

Meeting the PCI Data Security Standard

A Solidcore White Paper



Contact

Email: sales@solidcore.com

Web: <http://www.solidcore.com>

Tel: 888.210.6530

© 2005 Solidcore Systems. Solidcore

Systems, Solidcore and Solidification are trademarks of Solidcore Systems, Inc. All rights reserved in the United States and internationally.

