

CONTENTS OF THIS WHITE PAPER

---

Overview .....1

Background .....1

Who Needs To Comply .....1

What Is Considered Sensitive Data .....2

What Are the Costs/Risks of Non-Compliance .....2

How Varonis Helps With PCI Compliance.....3

Varonis DatAdvantage.....5

Varonis DataPrivilege .....5

## Varonis Systems & The Payment Card Industry Data Security Standard (PCI DSS)

### OVERVIEW

This document gives a brief overview of the PCI DSS basics and summarizes how Varonis data governance solutions can help organizations achieve compliance with a portion of the PCI DSS requirements.

### BACKGROUND

The PCI DSS was developed as part of a collaboration by MasterCard Worldwide, Visa International, American Express, Discover Financial Services and JCB. Their efforts have culminated in the standard that serves as directive and guideline to help organizations that deal in credit card information and processing prevent the misuse of this data.

### WHO NEEDS TO COMPLY

All merchants and service providers who store, process and transmit credit card information must undergo quarterly self-assessments as well as audits conducted over the Internet (vulnerability scans) by an Approved Scanning Vendor (ASV) and in accordance with PCI DSS Scanning Procedures.

Large merchants (i.e. more than 6 million transactions per year for all outlets including e-commerce) and service providers (i.e. more than 1 million transactions per year) must also undergo annual on-site audits performed by a PCI DSS Qualified Security Assessor (QSA). The audit is inclusive of all systems, applications and technical measures, as well as policies and procedures used in the storing, processing and transmission of cardholder and credit card information.

## WHAT IS CONSIDERED SENSITIVE DATA

Per the standard, the following information is considered sensitive:

- Primary Account Number (PAN)
- Cardholder name
- Service code
- Expiration date
- Pin Verification Value (PVV)
- Security code (3 or 4 digit)

In accordance with the standard, merchants or service providers are not allowed to store the PVV or the security code that uniquely identifies the piece of plastic in the cardholder's possession at the time of the transaction. However, the PAN, cardholder name, service code and expiration date may be stored.

## WHAT ARE THE COSTS/RISKS OF NON-COMPLIANCE

Credit card fraud and misuse reaches into the billions of dollars annually. While the costs per incident may vary by merchant size, they include:

- Loss of income from fraudulent transaction
- Cost to reissue cards
- Costs of investigation and possible litigation
- Possible fines imposed by credit card companies
- Loss of reputation, customer confidence and business
- Possible loss of ability to accept credit cards for payment

## HOW VARONIS HELPS WITH PCI COMPLIANCE

Varonis provides a comprehensive system for visibility, access control and auditing of unstructured data – the information that resides outside of databases. In fact, Varonis is the only vendor with a system for automating need-to-know based access to and holistic auditing of unstructured data. In the case of PCI, it is important to protect not only databases, but file shares as well. When file shares contain any of the PCI-designated sensitive information, organizations need to audit access to these shared networked resources as part of their PCI compliance efforts.

Many organizations naturally focus efforts for protecting cardholder information within databases, a challenge for which technical solutions abound. However, as breaches like Citigroup's<sup>1</sup> and Pfizer's have shown, enterprises are challenged to control access and dissemination of the spreadsheets and documents that might contain cardholder information. And the exporting of this sensitive cardholder data out of databases is all too common, so that the information may be analyzed as part of market research or be imported to other applications. In fact, 42 percent of enterprises hold customer data in spreadsheets as a matter of course according to Ventana Research<sup>2</sup>, and these figures don't include the individual users who conduct such exports on their own for business analytics or other purposes.

For this reason, it is important that enterprises not neglect their file shares when it comes to implementing technology for achieving PCI compliance.



**How Varonis Helps with PCI Compliance Continued**

PCI REQUIREMENTS <sup>3</sup>	VARONIS DATADVANTAGE	VARONIS DATAPRIVILEGE
Requirement 1: Install and maintain a firewall configuration to protect cardholder data		
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters		
Requirement 3: Protect stored cardholder data	√	√
Requirement 4: Encrypt transmission of cardholder data across open, public networks		
Requirement 5: Use and regularly update anti-virus software		
Requirement 6: Develop and maintain secure systems and applications		
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		
Requirement 10: Track and monitor all access to network resources and cardholder data	√	
Requirement 11: Regularly test security systems and processes	√	√
Requirement 12: Maintain a policy that addresses information security		√

## VARONIS DATADVANTAGE

Varonis makes the platform and applications that actualize data governance. The Varonis DatAdvantage software solution aggregates user, data and access event information from directories and file servers. Sophisticated analytics applied to the collected information show detailed data use and determine rightful access based on business need. Specifically, and in a non-intrusive way, Varonis:

- Protects data by recommending removal of overly permissive access controls
- Restricts unstructured data access to those with a business need for that data
- Tracks and monitors every user's every file touch
- Re-computes access controls to account for changes in roles and file server contents

## VARONIS DATAPRIVILEGE

DataPrivilege makes it possible to transition the responsibility of data entitlement management from IT to business owners without any infrastructure changes or business disruption. DataPrivilege brings together data owners and data users in a forum for communicating, authorizing and activating entitlements. Varonis DataPrivilege allows you to implement a cohesive data entitlement environment, thereby raising accountability and reducing risk. Upon implementation, DataPrivilege provides:

- Data protection by reducing errors in entitlement management
- Business need-to-know access control by enabling data owners to make the call
- Access approval rationale capture for refinement and improvement
- Policy and workflow enforcement for consistency and greater security

### Sources:

1. Citigroup Customer Data Leaked on LimeWire (2007): <http://www.eweek.com/c/a/Security/Citigroup-Customer-Data-Leaked-on-LimeWire/>
2. Organizations Struggle To Manage Customer Data As Information Assets (2007): <http://www.itbusinessedge.com/cm/community/features/guestopinions/blog/organizations-struggle-to-manage-customer-data-as-information-assets/?cs=22600>
3. PCI Data Security Standard (PCI DSS), PCI Security Standards Council: [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml)