PROTECTING CARDHOLDER DATA
Complying with
Payment Card Industry Standard Version 1.1

Notice

Copyright © 2006 - 2007 by Privacy Compliance Group, Inc.

Reproduction of all or any part of this document is permitted, but only for exclusive use within your company or organization. Any other reproduction of all or any part of this publication without the prior written permission of Privacy Compliance Group, Inc. (“PCG”) is prohibited.

PCG is a privacy and data protection consulting company that works with leading companies and government agencies on the effective use of personally identifiable information. Although PCG may employ licensed attorneys and accountants, the information in this paper is not intended to be legal or accounting advice. If your organization requires such advice, you should consult your own professional adviser.

If you have questions or would like additional information on the matters discussed in this paper, please contact Gary E. Clayton at gclayton@privacycg.com or via telephone at (214) 365-1665.

Privacy Compliance Group, Inc.
September 19, 2007
# Table of Contents

PROTECTING CARDHOLDER DATA .................................................................................................. 1  
INTRODUCTION ............................................................................................................................. 1  
WHY THE STANDARDS ARE IMPORTANT TO YOUR BUSINESS ............................................... 2  
WHEN DO THE PCI STANDARDS APPLY? ..................................................................................... 4  
WHAT does PCI VERSION 1.1 COVER? ......................................................................................... 4  
CARDHOLDER and SENSITIVE AUTHENTICATION DATA ........................................................... 5  
HOW VONTU PROTECTS CARDHOLDER and OTHER SENSITIVE DATA ............................... 7  
VONTU’S SOLUTION FOR PCI COMPLIANCE ............................................................................. 9  
HOW VONTU ENABLES COMPLIANCE WITH SPECIFIC VERSION 1.1 REQUIREMENTS ............ 10  
COMMONLY USED ELEMENTS of CARDHOLDER and SENSITIVE AUTHENTICATION DATA .... 12  
HOW TO GET STARTED WITH VONTU ....................................................................................... 15  
CONCLUSION ............................................................................................................................... 16  
ABOUT THE AUTHOR ................................................................................................................ 16
Protecting Cardholder Data

Complying with Payment Card Industry Data Security Standard 1.1

Introduction

It reads like a good legal thriller. Slowly and methodically, you are guided through a massive security breach. From the discovery of the crime, through the initial investigation, we read how a company struggles to get control of a massive data loss and determine what happened. We see the company as it moves from notification of law enforcement and government agencies to the ultimate disclosure to the public that data on over 45 million credit cards has been stolen. And, just when it seems that things are under control, we read in detail how massive and expensive litigation ensues throughout the United States, Canada and Puerto Rico – costing the company over $200 million in just six months. It’s a chilling account of what can happen when customer credit card information is not appropriately protected.

Sound like a new John Grisham novel? Unfortunately, this is not from the mind of a fiction writer. It’s the scenario portrayed in recent SEC filings¹ by TJX Companies (TJX), the parent of T.J. Maxx, Marshalls and other retailers. What is perhaps most interesting, however, is that TJX details what it knew—and what it didn’t know—about how and where its customer credit card data was being processed. TJX also seems to reveal that it failed to comply with some of the basic requirements of the Payment Card Industry (PCI) security standards by storing customer identification numbers.

The security breach involving TJX is perhaps the most visible of a growing number of incidents that bring home the message that companies must protect the data itself rather than relying upon network security. Companies must take a holistic view of security threats and protect sensitive data wherever it is stored or used. In order to accomplish this, companies must know where their data is located in order to comply with PCI and other standards.

In September 2006, the PCI’s Data Security Standard Version 1.1 (Version 1.1.)² was released, making changes in the requirements for protecting cardholder data. Version 1.1 makes a number of significant changes to the steps that companies must take to protect cardholder data. Perhaps the most significant aspect of Version 1.1 is its holistic approach to protecting cardholder data. While Version 1.0 emphasized reliance on encryption as the “ultimate protection mechanism,”³ Version 1.1 takes a more realistic and holistic approach. Version 1.1 now views encryption as a “critical component” of cardholder data protection. Version 1.1 requires companies to consider and implement other appropriate safeguards such as ensuring cardholder data is not stored unless absolutely necessary and not sending cardholder data in unencrypted e-mails.

This purpose of this paper is to discuss Version 1.1’s requirements for protecting cardholder data. This paper will also examine why implementing such safeguards is critical to you, your business and your customers. Finally, we will examine how Vontu’s Data Loss Prevention suite combines endpoint and network-based software to to prevent wrongful disclosure of confidential information while automatically enforcing data loss prevention policies wherever data is stored or used.

Why the Standards are Important to Your Business

A 2006 VISA CISP Bulletin⁴ pointed out the top five vulnerabilities in merchants’ efforts to protect cardholder data. The Bulletin states that the most common cause of data compromise is a merchant’s or service provider’s encoding of sensitive information on the card’s magnetic stripe in violation of the PCI Data Security Standard.⁵ The PCI Data Standard Version 1.1, section 3.2.1.4 explicitly prohibits the storage of the full contents of the magnetic stripe after the authorization process is completed. According to Visa, this information may be unknowingly stored because a “number of commercially available Point of Sale (POS) payment systems and custom-designed payment applications retain this data by default without any action by the user.” The PCI Standard also prohibits the storage of the Card Verification Value 2 (CVV2) and Personal Identification Numbers (PINs) or PIN blocks.

The VISA Bulletin candidly acknowledges that armed with such information, data hackers and identity thieves can cause significant damage.⁶ According to Visa:

With little effort, a duplicate card can be created that will appear indistinguishable from the original card during the authorization process. Mass storage of this data by merchants and agents exposes this sensitive information to potential compromise and can make it easy for hackers to commit fraud that is difficult for issuers to detect. CVV2 and PINs are also highly sought after by hackers and when compromised can expose the payment system to undue risks.⁷

Merchants and agents that fail to comply with the PCI Standard face potential fines⁸ from the major credit card companies as well as possible termination of their ability to process credit card transactions. In addition, merchants and agents face loss of reputation, significant brand damage and potential civil litigation by consumers and governmental agencies and departments.

TJX Litigation Proceedings

The litigation against TJX is a stark reminder of the torrent of legal problems that confront companies that improperly⁹ store credit card data and suffer security breaches. According to March 2007 10-K report, TJX currently faces the following legal actions:

- 7 putative class action lawsuits in Massachusetts
- 4 putative class action lawsuits in California


⁵ The improper storage of PINs appears to have been the main problem for TJ Maxx. In it’s 10-K Report, TJX states: We do not believe that customer identification numbers (PINs) were compromised, because, before storage on the Framingham system, they are separately encrypted. . . .” See TJX March 10-K. Under the PCI Security Standards, the PINs should not have been stored – encrypted or otherwise.


⁷ See TJX March 10-K.

⁸ Fines can range up to $500,000 for non-compliance and up to $100,000 per incident for failure to notify (Visa) of a suspected loss or theft.

⁹ This is alleged by plaintiffs in the related litigation against TJX. TJX has not specifically admitted violating the PCI standards, although a statement in its August 10-Q seems to indicate that it was storing credit card numbers in violation of the PCI standards. See Footnote 1, supra.
• 1 putative class action lawsuit in Alabama
• 1 putative class action lawsuit in Puerto Rico
• 6 putative class action lawsuits in Canada
• Lawsuit by the Arkansas Carpenters Pension Fund
• Ongoing investigations by the Attorneys General of approximately 30 states, the U.S. Federal Trade Commission, the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta and the Privacy Commissioner of British Columbia\(^\text{10}\)
• Litigation by the Massachusetts Bankers Association, Connecticut Bankers Association and individual banks (nearly 300 banks are involved in the litigation).

The cost of all this litigation is staggering. TJX reported that as of July 28, 2007, it had after-tax charges of approximately $118 million ($196 million pre-tax), or $0.25 per share, for the second quarter and $130 million\(^\text{11}\) ($216 million pre-tax), or \$0.27 per share, for the first six months with respect to the Computer Intrusion litigation.

TJX is not the first company to confront litigation and enforcement actions. In the last few years, dozens of security cases have been brought by the FTC against well-known names like Microsoft, DSW Shoe Warehouse, BJ’s Wholesale Club, ChoicePoint and CardSystems Solutions, Inc. Although the FTC’s legal authority for bringing the cases has varied, taken together, these cases all stand for the proposition that businesses that process consumer transactions must take appropriate measures to protect sensitive information.\(^\text{12}\)

In at least two of the higher profile cases, actions were brought against companies that failed to provide reasonable and appropriate security for consumer credit card data. As a result of their failure to provide reasonable and appropriate security, the companies incurred considerable negative press, expenses and potential civil liability. In the CardSystems case, for example, CardSyslems had security breaches affecting tens of millions of credit and debit cards.\(^\text{13}\) As a result, the company was required to implement comprehensive information security programs and independent third-party professional audits for 20 years. CardSystems also faced potential liability in the millions of dollars in private litigation for losses related to the breach.\(^\text{14}\) In the end, however, both Visa and American Express dropped CardSystems as a processor. The cumulative effect of these actions can be seen by a quick visit to the CardSystems’ Website. For a brief period of time, a short notice on the site revealed that the assets of CardSystems have been sold and the company has gone out of business.\(^\text{15}\) The Website has now been removed.

\(^\text{10}\) See TJX March 10-K.
\(^\text{11}\) See TJX August 10-Q.
\(^\text{12}\) See TJX March 10-K.
\(^\text{13}\) In the Matter of Card Systems Solutions, Inc. and Solutions Networks, Inc., d/b/a Pay by Touch Solutions, 052-3148 (February 23, 2006).
\(^\text{14}\) In addition to facing a massive class action suit, attorneys general from 48 states demanded CardSystems notify each of the more than 40 million consumers whose information was compromised. The National Association of Attorneys General (NAAG) demanded immediate remedial action by CardSystems and threatened litigation if their demands were not met. See, “States Want CardSystems to notify Consumers of Data Breach,” Consumer Affairs.com (June 23, 2005)[available at http://www.consumeraffairs.com/news04/2005/cardsystems_ag.html (visited September 20, 2007).
When Do the PCI Standards Apply?

One of the first distinctions noted between Version 1.0 and Version 1.1 is how they differ in determining their applicability. Version 1.0 applied to “all Members, merchants, and service providers that store, process or transmit cardholder data.” Version 1.1, however, states that it is applicable only if a “Primary Account Number (“PAN”)” is stored, processed, or transmitted. Conversely, Version 1.1 states that it does not apply if a PAN is not stored, processed or transmitted.

To determine if the PCI Standards apply to your business, simply ask if your company or organization takes any of the following actions with a PAN:

![Decision Tree Diagram]

The Version 1.1 Glossary defines the term PAN as “the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. Also called Account Number.”16 A PAN is important not only in determining the applicability of the standard, but also in determining what information must be protected by rendering it unreadable.17

What does PCI Version 1.1 Cover?

In order to determine what PCI Version 1.1 applies to, it is necessary to understand several key terms. Version 1.1 applies to all “system components.” System components are defined as any “network component, server, or application that is included in or connected to the ‘cardholder data environment.’” Version 1.1 defines the cardholder data environment as follows:

“[t]hat part of the network that possesses cardholder data, or sensitive authentication data. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment. Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliance, and other security appliances. Server types include but are not limited to the following: web, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS). Applications include all purchased and custom applications, including internal and external (Internet) applications.”

17 See, DSS Version 1.1, Requirement 3.4.
The PCI Standard does not define or explain what is meant by the term “posses,” although it apparently refers to storing, processing or transmitting cardholder data and/or sensitive authentication data. Unfortunately, the standard does not define or explain the terms “store,” “process” or “transmit.”

Cardholder and Sensitive Authentication Data

Version 1.1 applies to (1) cardholder data and (2) sensitive authentication data. It is, therefore, important to understand what personally identifiable data is included in these terms. The PCI Glossary defines “cardholder data” as:

- Full magnetic stripe or
- PAN plus any of the following:
  - Cardholder name
  - Expiration date
  - Service code

Sensitive authentication data, however, is not a term specifically defined in the PCI Glossary. Instead, Requirement 3.2 of the PCI Standard states that “sensitive authentication data” includes the data cited in Requirements 3.2.1 through 3.2.3. A review of these sections indicates that the following information is included as sensitive authentication data:

- **Full contents of any track from the magnetic stripe** on the back of a card. This data is alternatively called full track, track 1, track 2 and magnetic stripe data;

- **Card validation code or value** (CVC2/CVV2) (three-digit or four digit number printed on the front or back of a payment card) used to verify card-not-present transactions;

- **Personal Identification Number**; and

- **Encrypted PIN block**

---

18 For a definition of the term “processing”, see, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities of 23 November 1995 No L. 281 p. 31 which defines “processing” as: "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.”

19 The PCI Glossary does define “sensitive information or data” as “security-related information (for example, cryptographic keys, authentication data such as passwords, CVV, CVV2, complete track data and PINs) appearing in plaintext (sic) or otherwise unprotected form. Disclosure, modification, or destruction of this information could compromise the security of a cryptographic device, information system, or cardholder information or could be used in a fraudulent transaction.” See, PCI Data Security Standard Glossary, Abbreviations and Acronyms, available at https://www.pcisecuritystandards.org/tech/glossary.htm (visited September 20, 2007).
Putting these definitions together, to determine if the PCI Standard applies, you should ask:

**Does Your Company**

- Store
- Process
- Transmit

**PAN?**

If the Answer is YES, then Version 1.1 applies to:

<table>
<thead>
<tr>
<th>Cardholder Data Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Components</strong></td>
</tr>
<tr>
<td>• Firewall</td>
</tr>
<tr>
<td>• Switches</td>
</tr>
<tr>
<td>• Routers</td>
</tr>
<tr>
<td>• Wireless access points</td>
</tr>
<tr>
<td>• Network appliances</td>
</tr>
<tr>
<td>• Security appliances</td>
</tr>
<tr>
<td>• Web servers</td>
</tr>
<tr>
<td>• Database servers</td>
</tr>
<tr>
<td>• Authentication servers</td>
</tr>
<tr>
<td>• Mail servers</td>
</tr>
<tr>
<td>• Proxy servers</td>
</tr>
<tr>
<td>• Network Time Protocol servers</td>
</tr>
<tr>
<td>• Domain Name Servers</td>
</tr>
<tr>
<td>• Purchased applications</td>
</tr>
<tr>
<td>• Custom applications</td>
</tr>
<tr>
<td>• Internal applications</td>
</tr>
<tr>
<td>• External applications</td>
</tr>
</tbody>
</table>

**Version 1.1 applies regardless of the number of credit cards processed.**

There is a common misunderstanding of the requirements of PCI. The mistake arises because companies confuse the PCI’s categories for merchants and service providers based on the number of transactions they process. The PCI standards do not make a distinction in compliance requirements. The distinctions arise only with respect to what level of validation is required. The compliance requirements are the same – regardless of how many credit card transactions a merchant or service provider processes. As discussed above, PCI requires that any entity that stores, processes or transmits any credit card data must be in compliance with the PCI standards.
How Vontu Protects Cardholder and Other Sensitive Data

Companies can easily run into problems by failing to protect sensitive data wherever it is stored or used. The FTC’s case against BJ’s Wholesale Club20 illustrates this point. In its action, the FTC’s complaint noted that BJ’s Wholesale Club improperly stored sensitive data in files that were easily accessible, that were not encrypted or that had unrestricted access. Additionally, the case pointed out that applications might store such data on a network without the knowledge of the business.

The problem facing organizations is that they frequently do not know what sensitive customer or employee data they have or where it is stored throughout the enterprise. According to a recent survey, 64% of companies surveyed reported that they had never conducted an inventory of the sensitive customer data or employee data.21 Organizations simply cannot secure and manage what they cannot find.

In order to address these types of problems, PCI Standard Version 1.1 requires companies to protect sensitive data throughout its operations. The standard is comprised of twelve (12) requirements, which are organized into six logically related groups or “control objectives.” The objective of Version 1.1 is to ensure that Primary Account Number (PAN) and other cardholder and sensitive authentication data are protected throughout the environment in which they are used, transmitted and stored.

Vontu combines both endpoint and network-based software to protect cardholder data and other sensitive data wherever it is stored or used.

Stored Data

As the volume of data continues to grow within organizations, data security teams and business units have little or no visibility into where confidential data is stored across the enterprise. As a result, they are unable to protect such data against unauthorized access or transfer. Vontu’s Network Data Discovery and Protection (DDP) solution allows organizations to accurately “find and fix” exposed confidential or classified data on file servers, databases, desktops, laptops, and other data repositories.

Vontu Network Discover detects magnetic stripe, PAN and sensitive authentication data stored on file servers, databases, Microsoft® SharePoint®, Lotus® Notes®, Documentum®, LiveLink®, web servers, Microsoft® Exchange®, end-user laptops and desktops, and other data repositories. Vontu Network Protect then automatically protects (copy, delete, quarantine) information that violates the PCI standards.

Vontu is the only solution on the market that both discovers confidential data stored on the endpoint, and also prevents this data from inappropriately leaving the endpoint. As a result, PCI data stored on endpoints becomes visible so steps can be taken to remove, encrypt or relocate this data. Vontu can scan employee laptops and desktops to locate customer credit card information for a complete inventory of which laptops in which departments contain exposed PCI data. Vontu can also be used enterprise-wide to prioritize the rollout of full-disk encryption to higher-risk endpoints of the users that have the most confidential data.

Vontu Endpoint Discover provides agent-based scanning of stored data. With Vontu Endpoint Discover, you are able to have high-performance, parallel scanning of thousands of desktops and laptops, including offline machines and remote office systems, with only minimal network impact. Vontu Endpoint Discover can also scan

---


Page 7
the laptops of mobile employees who are frequently off the network (offline machines) for credit card numbers and magstripe data that is being stored in violation of PCI standards. Vontu Endpoint Discover also enables a company to scan laptops and desktops at branch offices with low bandwidth connection for stored cardholder data in violation of PCI standards.

Vontu Endpoint Discover addresses another potentially troublesome area: call center desktops. Vontu Endpoint Discover can scan hundreds of thousands of call center desktops simultaneously for a quick inventory of stored cardholder data, such as credit card numbers and magnetic stripe data that violate the PCI standards.

Data Usage

Organizations face similar problems with data usage. Since they do not always know how sensitive data is being used, they are unable to manage it. Vontu Network Data Monitoring and Prevention (DMP) solution monitors and prevents data loss on the network including email, IM, Web, Secure Web (HTTPS), FTP, P2P, and generic TCP.

Vontu Network Monitor detects unencrypted cardholder data across network protocols such as e-mail, web and secure web (HTTP over SSL), and file transfers (FTP).

Vontu Network Prevent then automates encryption by blocking communications or tagging e-mails for routing to an encryption gateway.

With an increasingly mobile workforce, organizations are confronted with the problem of effectively managing sensitive data on endpoints. Effective management requires the organization to know which laptops and desktops are storing exposed cardholder data. It is also crucial to know why confidential data is being sent from laptops when employees are working on and off the network. Finally, organizations must be able to manage what information is copied to USB and other portable storage devices such as CDs, DVDs and iPods®. Vontu Endpoint Prevent monitors and prevents cardholder data from being copied to USB, burnt to CD/DVD, downloaded to local drives, attached to network transmissions, or encrypted or concealed using high risk applications.

For example, if an employee or contractor copies confidential data or intellectual property to a USB drive that violates policy, Vontu detects the incident and notifies the data security team and/or management of the policy violation. Where appropriate, Vontu can also notify the employee or contractor of the violation. Vontu also provides you with the information you will need for compliance reporting.

Vontu provides PCI policy templates that are designed to facilitate your compliance with the PCI Standard. These templates assist in monitoring your network for all uses of cardholder and other sensitive data wherever it is stored or used. With Vontu Enforce Platform, organizations can automatically enforce universal Data Loss Prevention policies with a centralized platform for detection, remediation workflow, reporting, system management and security. Vontu’s ability to enforce policies can help drive employee behavior and lower costs of training and operations. Vontu can achieve this by automatically managing and scoring violations. Vontu can be configured to notify the sender or use of the cardholder data, as well as the managers or others on a need-to-know basis. Vontu’s user-friendly risk dashboard enables your company to immediately highlight areas of risk, thereby allocating your resources to the appropriate areas. Finally, Vontu’s automatic remediation reduces the use and proliferation of credit card data.
Vontu’s Solution for PCI Compliance

Vontu provides comprehensive PCI data loss prevention for any organization that stores and/or transmits Primary Account Number (PAN) and cardholder data. Specific Vontu capabilities include:

• **Pre-defined PCI policy template and data identifiers for PCI compliance**: Vontu’s PCI policy template contains pre-defined rules-based matching technology to safeguard PAN and cardholder data. The template also includes data identifiers for PCI compliance to detect and validate a wide range of sensitive data types such as PAN, magnetic stripe data, and bank identification numbers (BINs).

• **Discover and protect PAN and cardholder stored data**: Vontu enables organizations to discover and protect exposed PAN and cardholder data, as well as sensitive authentication data that may not be stored, on laptops, desktops, shared servers, and web servers and protect it through automatic policy enforcement by quarantining the file or moving it to an encrypted file share.

• **Monitor and prevent PAN and cardholder data usage**: Vontu enables organizations to monitor PAN and cardholder data usage across network protocols such as email, IM, Web, Secure Web (HTTP over SSL), FTP, P2P, and generic TCP, and automatically enforce policies to prevent PAN or cardholder data loss by blocking communications or tagging emails routing them to an encryption gateway.

• **Gain control and visibility into PAN and cardholder data on endpoints**: Vontu monitors and prevents PAN and cardholder data from being copied to USB, burnt to CD/DVD, downloaded to local drives, attached to network transmissions, or encrypted or concealed using high risk applications.

• **Comprehensive PCI compliance reporting and audit support**: Vontu provides pre-built PCI compliance reports and role-based dashboards that enable compliance teams to address internal and external audits.

• **Database encryption for PAN and cardholder data**: Only Vontu encrypts incident storage as required for PCI compliance. Original messages and matches to data loss policies within the messages are encrypted by the Vontu application before being stored in the database. Incidents are never stored on disk in clear text, including initial detection on servers and endpoint agents.

• **Automatic PCI policy enforcement and education**: Vontu automates PCI policy enforcement through auto-response and manager notifications that help organizations change employee behavior and pinpoint compliance gaps in existing business processes.

• **Role-based access control**: Vontu’s Role-Based Access Control displays Access Control List (ACL) and ownership information for unprotected cardholder stored data to audit and reinforce access controls. Additionally, Vontu’s Role-Based Access Control restricts access to detected cardholder data on a need-to-know basis. Vontu workflow and response rules empower business units and departments to review and remediate only those PCI incidents relevant to their role and privileges. These features help organizations demonstrate compliance with PCI DSS Requirements 7.1 and 7.2, which mandate a mechanism to automatically deny information access to any individual not specifically authorized.
How Vontu Enables Compliance with Specific Version 1.1 Requirements

The following table provides a summary of the PCI Standard’s requirements and control objectives. The table also provides an explanation of how Vontu helps achieve compliance with the Requirements.

<table>
<thead>
<tr>
<th>Control Objective</th>
<th>Standard</th>
<th>How Vontu Supports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Build and Maintain a Secure Network</strong></td>
<td><strong>Requirement 1:</strong> Install and maintain a firewall configuration to protect cardholder data.</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td><strong>Requirement 2:</strong> Do no use vendor-supplied defaults for system passwords and other security parameters.</td>
<td></td>
</tr>
<tr>
<td><strong>Protect Cardholder Data</strong></td>
<td><strong>Requirement 3:</strong> Protect stored cardholder data.</td>
<td>• Vontu Network Discover identifies stored unprotected cardholder data on file servers, databases, SharePoint, Lotus Notes, Documentum, LiveLink, web servers, Microsoft Exchange, end-user laptops and desktops, and other data repositories and Vontu Network Protect automatically protects (copy, delete, quarantine) information that violates standards. (Requirement 3.2)</td>
</tr>
<tr>
<td></td>
<td><strong>Requirement 4:</strong> Encrypt transmission of cardholder data across open, public networks.</td>
<td>• Vontu Network Discover detects magnetic stripe and PAN cardholder stored data. (Requirements 3.2 and 4.1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Vontu Network Monitor detects SMTP / HTTP / FTP / HTTP transmissions of Cardholder data. (Requirement 4.1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Vontu Network Prevent will automatically forward SMTP for encryption. (Requirement 4)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Vontu’s PCI Templates facilitate management of risk prevention and compliance with the standards. (Requirement 3.6)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Vontu helps keep cardholder data storage to a minimum. (Requirement 3.1)</td>
</tr>
<tr>
<td>Control Objective</td>
<td>Standard</td>
<td>How Vontu Supports</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Maintain a Vulnerability Management Program</td>
<td><strong>Requirement 5:</strong> Use and regularly update anti-virus software.</td>
<td>• Vontu enables automatic enforcement of your policies on the network and endpoints</td>
</tr>
<tr>
<td></td>
<td><strong>Requirement 6:</strong> Develop and maintain secure systems and applications.</td>
<td>• Vontu’s comprehensive monitoring of data on the network and on the endpoints, coupled with its auditing and reporting capabilities, enhance your risk management program and allow you to effectively measure your progress over time</td>
</tr>
<tr>
<td>Implement Strong Access Control Measures</td>
<td><strong>Requirement 7:</strong> Restrict access to cardholder data by business need-to-know.</td>
<td>• Vontu Role-Based Access and Control restricts access to detected cardholder data on a need-to-know basis.</td>
</tr>
<tr>
<td></td>
<td><strong>Requirement 8:</strong> Assign a unique ID to each person with computer access.</td>
<td>• Vontu Network Discover includes ACL information for cardholder stored data.</td>
</tr>
<tr>
<td></td>
<td><strong>Requirement 9:</strong> Restrict physical access to cardholder data.</td>
<td>• Vontu automatically redacts cardholder data, thereby limiting visibility yet providing remediation control via Vontu workflow and response rules.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cardholder data that is captured by Vontu is encrypted and, therefore, complies with Requirement 3.</td>
</tr>
<tr>
<td>Regularly Monitor and Test Networks</td>
<td><strong>Requirement 10:</strong> Track and monitor all access to network resources and cardholder data.</td>
<td>N/A</td>
</tr>
<tr>
<td>Control Objective</td>
<td>Standard</td>
<td>How Vontu Supports</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Requirement 11</strong>: Regularly test security</td>
<td><strong>Requirement 12</strong>: Maintain a policy that addresses information security.</td>
<td>• Vontu Enforce Platform automatically enforces PCI-based policies.</td>
</tr>
<tr>
<td>systems and processes.</td>
<td></td>
<td>• Vontu Enforce Platform measures effectiveness of the policies over time.</td>
</tr>
<tr>
<td><strong>Maintain an Information Security Policy</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Commonly Used Elements of Cardholder and Sensitive Authentication Data

PCI Standard Version 1.1 provides a convenient table that illustrates commonly used elements of cardholder and sensitive information data. The table identifies whether storage of each data element is permitted or prohibited. The table also identifies if each data element must be protected. The table below provides similar information; however, it also identifies how Vontu helps you achieve compliance with Version 1.1’s requirements for data storage and protection.

<table>
<thead>
<tr>
<th>Data Category</th>
<th>Data Element</th>
<th>Storage Permitted</th>
<th>Protection Required</th>
<th>PCI DSS Reg. 3.4</th>
<th>How Vontu Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cardholder</strong></td>
<td><strong>Primary Account Number (PAN)</strong></td>
<td><strong>YES</strong></td>
<td><strong>YES</strong></td>
<td><strong>YES</strong></td>
<td>• Vontu Network Discover identifies magnetic strip, PAN or other cardholder data that is stored on file servers, databases, SharePoint, Lotus Notes, Documentum, LiveLink, web servers, Microsoft Exchange, end-user laptops and desktops, and other data repositories. Vontu Network Protect then automatically protects and quarantines information that violates the PCI Standard</td>
</tr>
<tr>
<td><strong>Data</strong></td>
<td><strong>Data Element</strong></td>
<td></td>
<td></td>
<td></td>
<td>• Vontu Endpoint Prevent continuously monitors and prevents magnetic stripe, PAN or other cardholder data from being copied to USB drives, CD/DVD, iPods, and other removable media or downloaded to local drives in violation of policies</td>
</tr>
<tr>
<td></td>
<td><strong>Storage Permitted</strong></td>
<td></td>
<td></td>
<td></td>
<td>• Vontu displays access control and ownership information for any file containing confidential data to audit and reinforce access controls.</td>
</tr>
<tr>
<td></td>
<td><strong>Protection Required</strong></td>
<td></td>
<td></td>
<td></td>
<td>• Vontu Network Monitor detects SMTP / HTTP / FTP / HTTP transmissions of Cardholder data. (Requirement 4.1)</td>
</tr>
<tr>
<td>Data Category</td>
<td>Data Element</td>
<td>Storage Permitted</td>
<td>Protection Required</td>
<td>PCI DSS Req. 3.4</td>
<td>How Vontu Safeguards</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------</td>
<td>-------------------</td>
<td>---------------------</td>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Cardholder Name*</td>
<td>YES</td>
<td>YES *</td>
<td>NO</td>
<td>1. Vontu Network Prevent will automatically forward SMTP for encryption. (Requirement 4)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2. Vontu identifies cardholder names or other cardholder data that is stored on file servers, databases, SharePoint, Lotus Notes, Documentum, LiveLink, Microsoft Exchange, web servers, end-user laptops and desktops, and automatically protects and quarantines information that violates the PCI Standard.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3. Vontu continuously monitors cardholder names or other cardholder data being copied to USB drives, CD/DVD, iPods, and other removable media or downloaded to local drives. Vontu prevents confidential data from leaving an endpoint while still enabling legitimate usage of endpoint devices, removable media, or applications.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4. Vontu will detect and prevent SMTP / HTTP / FTP / HPSS transmission of cardholder names and can prevent it leaving your firewall.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5. Vontu will automatically forward SMTP for encryption.</td>
</tr>
<tr>
<td>Service Code*</td>
<td>YES</td>
<td>YES *</td>
<td>NO</td>
<td></td>
<td>1. Vontu identifies Service Codes or other cardholder data that is stored on file servers, Lotus Notes databases, desktops, laptops and automatically protects and quarantines information that violates the PCI Standard.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2. Vontu continuously monitors Service Codes or other cardholder data being copied to USB drives, CD/DVD, iPods, and other removable media or downloaded to local drives.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4. Vontu will detect and prevent email, IM, Web, Secure Web, HTTP over SSL, FTP, P2P and generic TCP transmission of service codes and can prevent it leaving your firewall.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5. Vontu will automatically forward SMTP for encryption.</td>
</tr>
<tr>
<td>Data Category</td>
<td>Data Element</td>
<td>Storage Permitted</td>
<td>Protection Required</td>
<td>PCI DSS Req. 3.4</td>
<td>How Vontu Safeguards</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------</td>
<td>-------------------</td>
<td>---------------------</td>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Expiration Date*</td>
<td>YES</td>
<td>YES *</td>
<td>NO</td>
<td>• Vontu identifies expiration dates or other cardholder data that is stored on file servers, desktops and laptops and automatically protects and quarantines information that violates the PCI Standard.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Vontu will detect and prevent email, IM, Web, Secure Web, HTTP over SSL, FTP, P2P and generic TCP transmission of expiration dates and can prevent it leaving your firewall.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Vontu will automatically forward SMTP for encryption.</td>
</tr>
<tr>
<td>Sensitive Authentication Data **</td>
<td>Full Magnetic Stripe</td>
<td>NO</td>
<td>N/A</td>
<td>N/A</td>
<td>• Vontu identifies full magnetic stripe data, CV2, CVV2, CID, PIN and/or PIN Block numbers, or other cardholder data that is stored on file servers, databases, SharePoint, Lotus Notes, Documentum, LiveLink, web servers, Microsoft Exchange, and end-user laptops and desktops and automatically protects and quarantines information that violates the PCI Standard.</td>
</tr>
<tr>
<td></td>
<td>CVC2/CVV2/ CID</td>
<td>NO</td>
<td>N/A</td>
<td>N/A</td>
<td>• Vontu continuously monitors full magnetic stripe data, CV2, CVV2, CID, PIN and/or PIN Block numbers, or other cardholder data being copied to USB drives, CD/DVD, iPods, and other removable media or downloaded to local drives.</td>
</tr>
<tr>
<td></td>
<td>PIN / PIN Block</td>
<td>NO</td>
<td>N/A</td>
<td>N/A</td>
<td>• Vontu will detect and prevent email, IM, Web, Secure Web, HTTP over SSL, FTP, P2P and generic TCP transmission of these data elements and can prevent it leaving your firewall.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Vontu will automatically forward SMTP for encryption.</td>
</tr>
</tbody>
</table>

* NOTE: These data elements must be protected if stored in conjunction with PAN.

**NOTE:** Sensitive authentication data must not be stored subsequent to authorization – even if encrypted.
How to Get Started With Vontu

Vontu’s team of Data Loss Prevention experts will work with you to understand your unique data security requirements, priorities, and share insight into our industry best practices. Contact Vontu to get started at +1.415.464.8100 or email at info@vontu.com.

Vontu is Proven Market Leader

Vontu’s effective approach to Data Loss Prevention has made it a market leader. Vontu is also the proven choice of leading companies:

- Vontu has 60% Data Loss Prevention market share
- One in five FORTUNE 100 companies rely upon Vontu.
- More FORTUNE 500 customers in deployment than any other vendor
- Only integrated Data Loss Prevention suite that combines endpoint and network-based software to prevent the loss of confidential data wherever it is stored or used
- Only Endpoint solution with the ability to both Discover and Prevent confidential data loss at the endpoint
- Only vendor with Network Data Discovery and Protection native coverage of key data repositories including SharePoint, SQL databases, Microsoft Exchange, Lotus Notes, Documentum, and LiveLink
- Broadest range of automated stored Data Protection actions including file quarantine, relocation and collection
- Highest accuracy with TrueMatch™ detection technology across network and endpoint products
- Proven enterprise FORTUNE 100 scalability across products
- Only workflow that is automated, prioritized, and correlated
- Only Data Loss Prevention solution to support cross suite, multi-dimensional, ad-hoc incident reporting analytics (e.g., group by quarter, then by business unit, then by severity)

About Vontu

Vontu, now part of Symantec, is the leading provider of Data Loss Prevention solutions that combine endpoint and network-based technology to accurately detect and automatically protect confidential data wherever it is stored or used. By reducing the risk of data loss, Vontu solutions from Symantec help organizations ensure public confidence, demonstrate compliance and maintain competitive advantage. Vontu Data Loss Prevention customers include many of the world’s largest and most data-driven enterprises and government agencies. Vontu products have received numerous awards, including IDG’s InfoWorld 2008 Technology of the Year Award for “Best Data Leak Prevention,” as well as SC Magazine’s 2006 U.S. Excellence Award for “Best Enterprise Security Solution” and Global Award for “Best New Security Solution.” For more information, please visit http://go.symantec.com/vontu.
Conclusion

A Visa International survey of more than 6,000 consumers across 12 countries, conducted following some of the recent high-profile data breaches, found that data security was a major concern for 64% of the respondents. The survey also found that consumers have begun changing their behavior due to fears of identity theft and misuse of their information. The Visa International survey found that 24% of those surveyed reported that they were now limiting their use of online shopping sites. In a survey by the Ponemon Institute, 58% of consumers who had received a letter notifying them of a data breach said it had decreased their trust and confidence in the organization. Nineteen percent said they immediately terminated their accounts with vendors who lost their information; 40% considered taking their business elsewhere; and 5% said they hired lawyers.

Avoiding these types of risks and complying with the PCI Data Security Standard requires a common sense approach and appropriate administrative, physical, technical measures and safeguards to protect cardholder data. Effective and ongoing management of your customers’ cardholder data requires cost-effective and powerful tools to enable automatic compliance with your company's policies and data processing procedures. Vontu provides powerful technology that can help you avoid losing 19% of your customers immediately after a data breach incident. It can also help you protect against the risk of 40% of your customers considering taking their business elsewhere after a data breach. And finally, and perhaps as importantly, it can help you avoid the prospect of having to confront the 5% who hired lawyers because of a data breach.

About the Author

Gary Clayton is the founder and CEO of Privacy Compliance Group, Inc., a leading privacy and data protection consulting company. Privacy Compliance Group works with companies and government agencies to establish effective privacy compliance programs and to develop practices and policies to comply with privacy laws around the globe. Additional information is available at www.privacycg.com.

Gary Clayton has worked with leading multinational companies and with numerous agencies of the US Government, including the Department of Homeland Security, the Department of Transportation, the General Accounting Office and the Federal Trade Commission. He has extensive experience in all aspects of privacy and has been actively involved in working with clients in over 55 countries. Mr. Clayton has worked in the EU and assisted the US Department of Commerce in negotiations with the EU on the Safe Harbor agreement and the Department of Homeland Security in negotiations regarding access to passenger data.

Mr. Clayton is an attorney who is admitted to practice in Washington, D.C., Texas and Louisiana. He has lived and studied in Europe where he received an advanced law degree (LLM) in European and International Law from the University of Exeter, England. He has also studied comparative legal systems at the Université de St. Domaine, Grenoble, France. Mr. Clayton received an M.A. in International Law and Organizations from the School of International Service, the American University, Washington, D.C. He received his B.A. and J.D. from Louisiana State University. He is a frequent author and speaker on global privacy and data protection issues. He can be contacted at gclayton@privacycg.com or +1.214.365.1665.

---

24 Id.
25 Id.