

Cardholder Information Security Program (CISP)

Payment Application Best Practices

Overview

Version 1.0

INTRIX Systems Group, Inc.
2260 Douglas Blvd., Suite 240
Roseville, CA 95661
Phone: (916) 577-1315
Fax: (916) 577-1316
Contact: supersupport@intrix.com

Overview

The following document is designed to give users of the Transcend™ application an outline of the recently implemented security policies in the payment processing industry. The document summarizes the evolution of today's standards, describes the industry best practices for payment applications and then instructs users of the Transcend™ application in areas not completely controlled by the payment application but necessary to implement the product in a CISP compliant manner.

All the information contained in this document is either paraphrased or copied verbatim from the Visa CISP site at:

http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html?ep=v_sym_cisp.

History

Visa first introduced the Cardholder Information Security Program (CISP) in 2001. MasterCard was quick to follow suite with their Security Program called Site Data Protection Plan (SDP). Nearly four years later the industry has now evolved into a single standard endorsed by nearly every payment industry participant.

Visa's Cardholder Information Security Program (CISP)

CISP is the acronym for Visa's Cardholder Information Security Program, and if you store, transmit, or process Visa cardholder data, then CISP does apply to you. By implementing CISP, Visa is placing the responsibility of protecting Visa cardholder data on everyone involved in the transaction process.

How CISP Compliance Works

CISP compliance is required of all merchants and service providers that store, process, or transmit Visa cardholder data. The program applies to all payment channels, including retail (brick-and-mortar), mail/telephone order, and e-commerce. To achieve compliance with CISP, merchants and service providers must adhere to the Payment Card Industry (PCI) Data Security Standard, which offers a single approach to safeguarding sensitive data for all card brands. This Standard is a result of collaboration between Visa and MasterCard and is designed to create common industry security requirements, incorporating the CISP requirements. Other card companies operating in the U.S. have also endorsed the PCI Data Security Standard within their respective programs.

Using the PCI Data Security Standard as its framework, CISP provides the tools and measurements needed to protect against cardholder data exposure and compromise across the entire payment industry. The PCI Data Security Standard consists of twelve basic requirements supported by more detailed sub-requirements:

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored data
4. Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

CISP Compliance Validation

Separate and distinct from the mandate to comply with CISP requirements is the validation of compliance. It is a fundamental and critical function that identifies and corrects vulnerabilities, and protects customers by ensuring that appropriate levels of cardholder information security are maintained. Visa has prioritized and defined levels of CISP compliance validation based on the volume of transactions, the potential risk, and exposure introduced into the Visa system by merchants and service providers.

Compliance Validation Details and Deadlines

Acquirers are responsible for ensuring that all of their merchants comply with CISP, however, merchant compliance validation has been prioritized based on the volume of transactions, the potential risk, and exposure introduced into the Visa system.

Merchant Levels Defined

Acquirers are responsible for determining the compliance validation levels of their merchants. All merchants will fall into one of the four merchant levels based on annual Visa transaction volume. The transaction volume is based on the aggregate number of Visa transactions from a Doing Business As (DBA) or a chain of stores (not of a corporation that has several chains). Merchant levels are defined as:

Merchant Level	Description
1	<ul style="list-style-type: none"> • Any merchant-regardless of acceptance channel-processing over 6,000,000 Visa transactions per year. • Any merchant that has suffered a hack or an attack that resulted in an account data compromise. • Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system. • Any merchant identified by any other payment card brand as Level 1.
2	<ul style="list-style-type: none"> • Any merchant processing 150,000 to 6,000,000 Visa e-commerce transactions per year.
3	<ul style="list-style-type: none"> • Any merchant processing 20,000 to 150,000 Visa e-commerce transactions per year.
4	<ul style="list-style-type: none"> • Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants processing up to 6,000,000 Visa transactions per year.

CISP Compliance Validation Basics

In addition to adhering to the twelve security requirements and sub-requirements, compliance validation is required for Level 1, Level 2, and Level 3 merchants, and strongly recommended for Level 4 merchants.

Level	Validation Action	Validated By	Due Date
1	<ul style="list-style-type: none"> • Annual On-Site Security Audit <li style="text-align: center;">& • Quarterly Network Scan 	<ul style="list-style-type: none"> • Independent Security Assessor or Internal Audit if signed by Officer of the company • Qualified Independent Scan Vendor 	9/30/04
2 and 3	<ul style="list-style-type: none"> • Annual Self-Assessment Questionnaire <li style="text-align: center;">& • Quarterly Network Scan 	<ul style="list-style-type: none"> • Merchant • Qualified Independent Scan Vendor 	6/30/05
4*	<ul style="list-style-type: none"> • Annual Self-Assessment Questionnaire (Recommended) <li style="text-align: center;">& • Network Scan (Recommended) 	<ul style="list-style-type: none"> • Merchant • Qualified Independent Scan Vendor 	TBD

*Level 4 merchants must comply with CISP; however, compliance validation for merchants in this category will be determined at the acquirer's discretion.

MasterCard's Site Data Protection Plan (SDP)

MasterCard's Site Data Protection Program (SDP). SDP provides a comprehensive approach to evaluating and improving web site security. The SDP Program provides acquiring members with the ability to deploy security compliance programs, ensuring that online merchants and Member Service Providers are adequately protected against hacker intrusions and account data compromises.

The SDP Program includes the following elements:

The MasterCard Security Standard

A series of manuals providing security requirements and best practices for participating acquiring members, online merchants, Member Service Providers, and data security vendors.

Evaluation Tools

Participants can demonstrate MasterCard Security Standard compliance by using the MasterCard Security Self-Assessment and Network Scanning Tools. With these tools, participants can self-evaluate their security situation and conduct real-time vulnerability assessments of their web infrastructure.

SDP Service

The MasterCard Site Data Protection Service is a proactive, cost-effective, global solution offered by MasterCard through its acquiring members. The SDP Service includes network vulnerability scans and alert services offered by their SDP Service partner, Ubizen.

Alternative Vendor Solutions

As an alternative to the SDP Service, participants may select any security vendor solution that is compliant with MasterCard Security Standard. If desired, acquirers can ensure vendor compliance through the use of an optional, fee-based vendor certification program offered by MasterCard.

Web Insurance

An optional, discounted Marsh insurance policy, offering financial protection in case of a compromise is available.

Payment Card Industry Data Security Standard

The Payment Card Industry (PCI) Data Security Standard offers a single approach to safeguarding sensitive data for all card brands. This Standard is a result of the collaboration between Visa and MasterCard and is designed to create common industry security requirements, incorporating the CISP requirements. Other card companies operating in the U.S. have also endorsed the PCI Data Security Standard within their respective programs.

PCI Data Security Standard Basic Requirements

The PCI Data Security Standard consists of twelve basic requirements supported by more detailed sub-requirements:

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored data
4. Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

Payment Application Best Practice

The following has been taken directly from the Visa/CISP web site. Visa has developed *Payment Application Best Practices* to address security and the risks associated when full magnetic stripe data or CVV2 values are stored after authorization by payment applications. The best practices assist software vendors in creating secure payment applications that help ensure merchant CISP compliance.

Best Practices Goal

The goal of the *Payment Application Best Practices* is to help software vendors create secure payment applications. To be considered secure, these applications must not retain full magnetic stripe data or CVV2 data and must support a merchant's ability to comply with CISP requirements. Acquirers are responsible for ensuring that their merchants and service providers confirm the security of their payment applications using the *Payment Application Best Practices*.

Visa Recommendations

Visa has been actively working to educate software vendors and to provide best practices for secure payment applications where sensitive track data and CVV2 values are never stored subsequent to authorization. **Visa strongly recommends that:**

Software vendors validate their payment applications against recommendations outlined in *Visa's Payment Application Best Practices*. Visa makes no endorsement of applications or products and disclaims all warranties. Members remain responsible for performing their own evaluation and due diligence to ensure CISP compliance of their merchants and service providers.

Acquirers share the *Payment Application Best Practices* with both card-present and online merchants, and encourage them to use it to evaluate their current payment applications, as well as any pending payment application implementation. Acquirers and merchants can also encourage software vendors to participate in Visa's validation effort. Acquirers refer to Visa's List of CISP-Validated Payment Applications and encourage their merchants to use CISP-validated payment applications. .

Validation Procedures and Documentation

Software vendors seeking to validate their payment applications must engage a Visa-qualified independent security assessor to perform an on-site review and submit the required documentation to Visa. Compliance validation takes place at software vendor's expense, as follows:

The *Annual On-Site Security Audit* must be completed according to the *Payment Application Best Practices* document. This document is also to be used as the template for the Report on Validation. The scope of CISP validation is described in the *Payment Application Best Practices* download.

Assessors performing payment application reviews must contact Visa for approval before proceeding with the audit specified in the *Payment Application Best Practices*. Visa will not accept audits without this pre-approval.

Payment Application Best Practices Summary

The following are the high level best practices to follow in order to insure the Payment Application complies with the *Payment Application Best Practices* document. Each high-level best practice has several additional elements that are tested during the certification process. The requirements for Payment Application Best Practices validation are derived from the Payment Card Industry (PCI) Data Security Standard and the PCI Security Audit Procedures. These documents, detail what is required to be CISP compliant (and therefore what a payment application should do to facilitate a merchant's CISP compliance) and should be used as a reference for CISP standards. Validated applications must be capable of being implemented in a CISP-compliant manner.

1. Do not retain full magnetic stripe or CVV2 data.
2. Protect stored data.
3. Provide secure password features.
4. Log application activity.
5. Develop secure applications.
6. Protect wireless transmissions.
7. Test applications to address vulnerabilities.
8. Facilitate secure network implementation.
9. Cardholder data must never be stored on a server connected to the Internet.
10. Facilitate secure remote software updates.
11. Facilitate secure remote access to the application.
12. Encrypt sensitive traffic over public networks.
13. Encrypt all non-console administrative access.

The purpose of this document is to summarize the recently implemented security policies in the payment processing industry. For more information and the latest information, readers are encouraged to visit:

http://usa.visa.com/business/accepting_visas_ops_risk_management/cisp.html?ep=v_sym_cisp.

This publication has been prepared and written by INTRIX Systems Group, Inc. (INTRIX) and is copyright. Other than for the purposes of and subject to the conditions prescribed under the Copyright Act, no part of it may in any form or by any means (electronic, mechanical, micro-copying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission from the document controller. Product or company names are trademarks or registered trademarks of their respective holders.

Note for non-INTRIX readers: The contents of this publication are subject to change without notice. All efforts have been made to ensure the accuracy of this publication. Notwithstanding, INTRIX does not assume responsibility for any errors nor for any consequences arising from any errors in this publication.

