

Payment Card Industry

Data Security Standard

INFORMATION SHEET

Publication Date: January 2007

CommSecure Australia Pty Limited
ABN 14 001 950 670

964 Pacific Highway
Pymble NSW 2073 Australia

Telephone: +61 2 9497 4400
Facsimilie: +61 2 9497 4499
Website: www.commsecure.com

This document is the property of CommSecure Australia Pty Limited (the "Company") and the information contained herein is protected by copyright. No part of this document may be reproduced in any form including photocopying, electronically or translation into a foreign language without the express written permission of the Company. Such unauthorised usage is a violation of Australian and International copyright law.

OVERVIEW

With the increasing use of credit cards for Internet payments, Visa, Mastercard and other payment card schemes have joined forces and developed a global industry standard for the secure management of credit card account information. Known as the Payment Card Industry (PCI) Data Security Standard (DSS), it addresses mitigating the risk of internet fraud associated with compromised credit card account information.

Prior to the establishment of PCI DSS, individual card schemes would mandate their own security standard, which not only meant that standards could vary significantly but they had become complex for merchants and financial institutions to monitor and support. PCI DSS eliminates the problem of adhering to multiple standards by establishing a single global standard.

Consumer Concerns

As part of a global research programme sponsored by Visa, it was found that the No. 1 concern among consumers worldwide (64%) is the loss or theft of personal and financial information. This surpasses other concerns such as terrorism (58%), job loss (57%), disease epidemics (55%) and natural disasters (46%).¹

PCI DSS was developed to apply security practices and standards to the way merchants, payments gateway providers and financial institutions capture, store and maintain credit card account information. It is an ongoing program that will require individual program participants to demonstrate compliance on a regular basis.

CommSecure's Commitment

CommSecure has been committed to the highest standards in online transaction security since its inception in 1999. Prior to the launch of PCI DSS, the company maintained a high level of security certification including DSD ACSI-33. The company is committed to the PCI DSS standard and is actively engaged in an ongoing implementation programme in conjunction with its sponsoring banks and credit card partners.

¹ Global Consumer Attitudes and Behaviors Toward Data Security, Visa International (www.visa.com)

FREQUENTLY ASKED QUESTIONS

What is the Payment Card Industry (PCI) Data Security Standard (DSS)? *

The PCI Data Security Standard represents a common set of industry tools and measurements to help ensure the safe handling of sensitive information for credit card payment processing.

Initially created by aligning Visa's Account Information Security (AIS)/Cardholder Information Security (CISP) programs with MasterCard's Site Data Protection (SDP) program, the standard provides an actionable framework for developing a robust account data security process - including preventing, detecting and reacting to security incidents.

What are the requirements that have to be satisfied to be in compliance with the PCI Data Security Standard? *

The PCI Data Security Standard is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

The PCI Data Security Standard is comprised of 12 general requirements designed to:

- Build and maintain a secure network;
- Protect cardholder data;
- Ensure the maintenance of vulnerability management programs;
- Implement strong access control measures;
- Regularly monitor and test networks; and
- Ensure the maintenance of information security policies.

How do I determine whether my business would be required to do a full independent assessment or a self assessment? *

Merchants that store payment account data should contact the acquiring financial institutions with whom they have merchant agreements to determine whether they must validate compliance and the specific requirements for compliance validation. Service providers should contact the individual payment brands for further information.

Where can I get more information about the exact requirements needed to be PCI DSS compliant? *

The PCI DSS standard and all supporting documentation can be found on www.pcisecuritystandards.org.

* Excerpts from www.pcisecuritystandards.org