GUIDELINES FOR SECURING CARDHOLDER DATA FOR YOUR ECOMMERCE WEBSITE

CONTENTS

WELCOME

As the digital world expands, the need to protect personal information has never been more important. Credit card information is highly valuable and continually sought after by fraudsters. Minimal investment and lack of IT Security can cause your business to be vulnerable in the online environment.

This document is a guideline to assist you with understanding the most appropriate payment solution for your website to ensure card data is secure. The document does not represent the full PCI DSS standard.

OVERVIEW

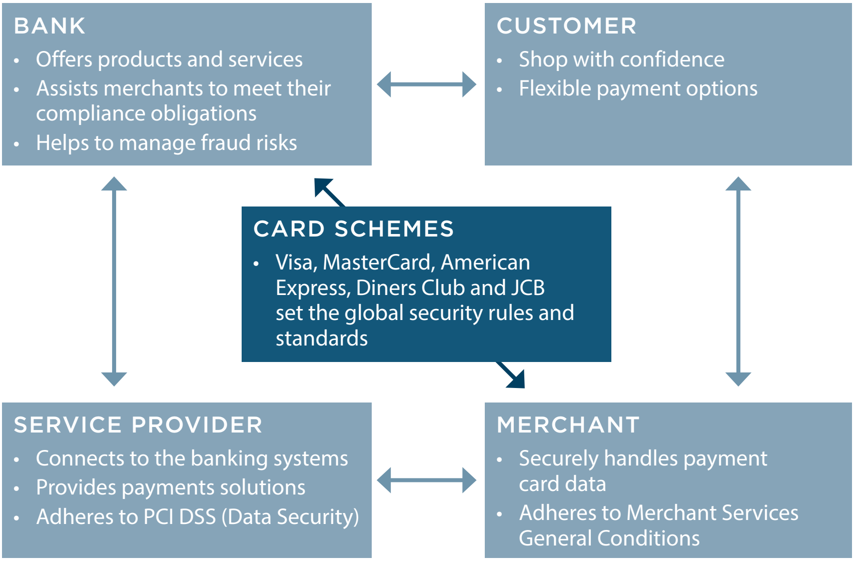
CARD PROCESSING SECURITY STANDARDS

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally.

PCI DSS is governed by the PCI Security Standards Council (PCI SSC) and is composed of card schemes such as Visa, MasterCard, American Express, Discover and JCB. The PCI SSC set the rules that define the minimum acceptable security standards and requirement for merchants and service providers. PCI DSS applies to all merchants that store, process or transmit Payment Card Data.

Your merchant agreement requires you to protect cardholder data and be PCI DSS compliant. You can reduce your security effort and investment by using solutions from service providers that are PCI DSS compliant.

ROLES AND RESPONSIBILITIES



BANK

- Offers products and services
- Assists merchants to meet their compliance obligations
- Helps to manage fraud risks

CUSTOMER

- Shop with confidence
- Flexible payment options

CARD SCHEMES

- Visa, MasterCard, American Express, Diners Club and JCB set the global security rules and standards

SERVICE PROVIDER

- Connects to the banking systems
- Provides payments solutions
- Adheres to PCI DSS (Data Security)

MERCHANT

- Securely handles payment card data
- Adheres to Merchant Services General Conditions

PAYMENT CARD INDUSTRY AND DATA SECURITY STANDARD (PCI DSS) PRINCIPLES AND REQUIREMENTS

To become PCI DSS compliant you need to ensure the following principles and requirements apply to your business.

The complete PCI DSS standard can be located via the PCI Security Standards Council website www.pcisecuritystandards.org/

PCI DSS Principles	PCI DSS Requirements
Build and Maintain a Secure Network	• Install and maintain a firewall configuration to protect data • Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	• Protect stored data by using methods such as lock and key, data masking or data encryption • Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	• Use and regularly update anti-virus software • Develop and maintain secure systems and applications
Implement Strong Access Control Measures	• Restrict access to data • Assign a unique ID to each person with computer access • Restrict physical access to cardholder data
Regularly Monitor and Test Networks	• Track and monitor all access to network resources and cardholder data • Regularly test security systems and processes
Maintain an Information Security Policy	• Maintain a policy that addresses information security

IMPORTANCE OF PROTECTING YOUR CUSTOMERS CARD INFORMATION

BENEFITS OF PROTECTING CARD INFORMATION

- Customers can shop with confidence
- Reduce business interruption with continuous payment acceptance
- Avoid unexpected IT costs to fix security gaps
- Protect your business reputation.

IMPACT OF NOT PROTECTING CARD INFORMATION

- Customers may find fraudulent transactions on their statement after shopping at your website
- Interrupted cash flow, with your bank likely to disable card payments upon detection of fraud
- Reputational damage
- Additional IT costs to resolve security gaps
- Card scheme fines may be imposed.

THE ROLE OF SERVICE PROVIDERS

Service providers provide payment solutions between your business and the bank, this includes shopping carts and payment gateways. You own the relationship and the agreement with the service provider.

Service providers can help to minimise your risk of exposing card information. Taking the time to research and select the right service provider up front could help to reduce your ongoing costs and need for future change.

Service providers that store, process, transmit or influence the security of cardholder data must be PCI DSS compliant. They must provide an Attestation of Compliance completed by an independent PCI DSS qualified security company annually.

Each service provider's responsibility will vary based on the level of services they offer. Not all products offered by these service providers reduce the risk of cardholder data being stolen from your website. Consult with your service provider about the products they offer where they are directly responsible for the protection of card data.

CARD PAYMENT PROCESSING SOLUTIONS

The following payment solutions can help protect cardholder information.

HOSTED SHOPPING CARTS

This solution is fully hosted by the service provider and incorporates your website and its card processing connectivity. The service provider is responsible for the entire solution and maintaining the software and the servers. Validated PCI compliant hosted shopping carts are fully outsourced and entirely responsible for the card processing security via these systems.

CUSTOM SHOPPING CARTS

Also known as 'proprietary or off the shelf carts', this type of software solution can be customised to meet your needs by a web developer. This solution must be installed on a web server or on a web host shared environment. You become responsible for the security of the solution.

Selecting the lowest risk payment gateway integration using the information guide below will help you protect card data in the online environment.

PAYMENT GATEWAYS

You can significantly reduce the risk of cardholder data theft by using a payment gateway to capture the cardholder information to process the payment. To ensure the payment gateway protects cardholder data, it must be PCI compliant.

Using a PCI compliant payment gateway does not make your website instantly secure, however using the payment gateway to capture the card details on its pages such as a Hosted Payment Page or iFrame, explained below, will ensure this risk is minimised.

We have set out payment gateway integration solutions below.

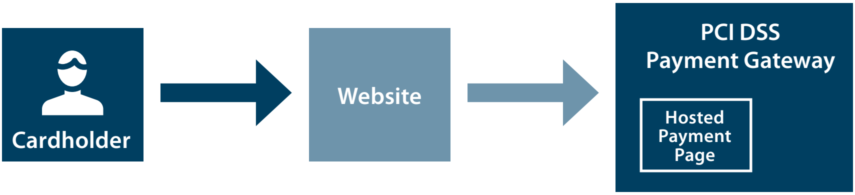
HOSTED PAYMENT PAGES

Hosted payment pages re-direct the customer to a different page from your website to enter the card information. This page is hosted by the payment gateway, which is responsible for the security of the cardholder data. Hosted payment pages may give you the ability to customise the background, text font and colour to fit in with your website.

The URL changes from your website to the payment gateway's URL providing shoppers with confidence the site is secure.

Characteristics of hosted payment pages include:

- The cardholder information is entered into the secured page hosted by the payment gateway
- Transaction details can be viewed via the payment gateway merchant portal
- Confirmation or decline of the transaction will come back to your website
- The payment gateway is responsible for the security of the cardholder data
- This option is considered to have the lowest level of risk if the payment gateway is PCI DSS compliant.



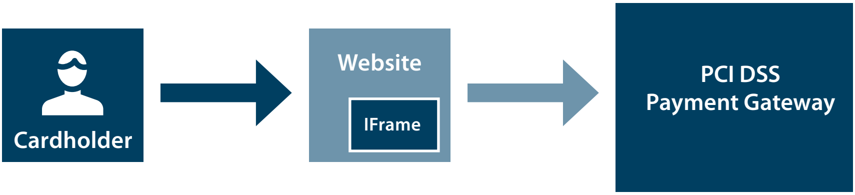
IFRAME (INLINE FRAMES)

iFrames allow a web page to be embedded within another web page, which is then populated with the cardholder information and secured by the payment gateway. This option allows you to maintain your website look and feel.

Should a website be compromised with an iFrame, you will be able to easily identify this within 1-2 days when funds are not being settled into your bank account.

Characteristics of iFrames include:

- The iFrame presents the payment gateway's page within your website and appears transparent to the end user
- Additional information can be passed to the payment gateway behind the scenes
- The payment gateway is responsible for the cardholder data
- This option is considered to have a very low level of risk; similar to the hosted payment page if the payment gateway is PCI DSS compliant.



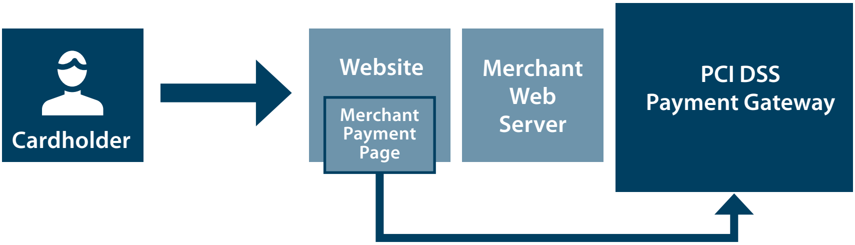
HYBRID INTEGRATION – ALSO KNOWN AS DIRECT POST OR TRANSPARENT REDIRECT

Hybrid Integrations ensure the cardholder information is sent directly from the customer's browser to the payment gateway. This solution aims to exclude your web server from the transaction flow and the risk of storing cardholder data. Your website maintains its look and feel and you have complete control over the entire page.

Should your website be compromised with a Hybrid Integration, detection may be difficult and card data may be sent to multiple places including the payment gateway. The scope of this risk is limited to your website payment page.

Characteristics of Hybrid Integration methods include:

- Cardholder data is entered into your website page making your website responsible for managing the security of the cardholder details
- The cardholder details do not pass through your web server or selected shared web host provider, reducing the number of systems involved in the card processing flow
- Security controls need to be implemented to eliminate fraudsters applying code to your page to extract cardholder data
- Security controls, such as a Web Application Firewall, Anti-Virus, Penetration Testing, Network Vulnerability Scans and File Integrity Monitoring should be implemented with this solution
- This option is regarded as medium level risk as the cardholder details don't flow through your web server or shared web host. Controls need to be put in place to reduce the security gaps.



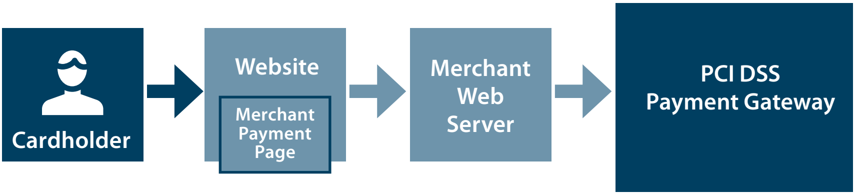
MERCHANT HOSTED API (APPLICATION PROGRAMMING INTERFACE)

Merchant Hosted API integrations involve your website capturing the cardholder details through to your web server and passing this to the payment gateway. This option places the responsibility onto you to ensure your website and the web server are secure.

Should your website be compromised with an API integration, detection is difficult and card data can be intercepted at any point between the website and your web server. Data in transit or stored data may be found by fraudsters. The scope of this risk is across all systems that card data passes through as well as any other connected networks.

Characteristics of API integration methods include:

- This option provides the most flexibility but also the most risk as you are responsible for protecting the cardholder data while it's in transit via your network
- The payment gateway is only responsible for the cardholder data once it receives it and not while it's in transit
- This option requires the most IT security investment. You are responsible for protecting the cardholder data
- This option has the highest level of risk of having cardholder details stolen by fraudsters.



SUMMARY OF PAYMENT GATEWAY SOLUTION OPTIONS

- Select the safest payment gateway solutions, taking into consideration your capability to implement IT security controls, the level of investment and desired functionality
- Ensure your service provider agreements refer to the PCI DSS
- Seek assistance from experts
- If in doubt, engage your bank for assistance
- Perform regular Network Vulnerability Scans and remediate any vulnerability discovered.

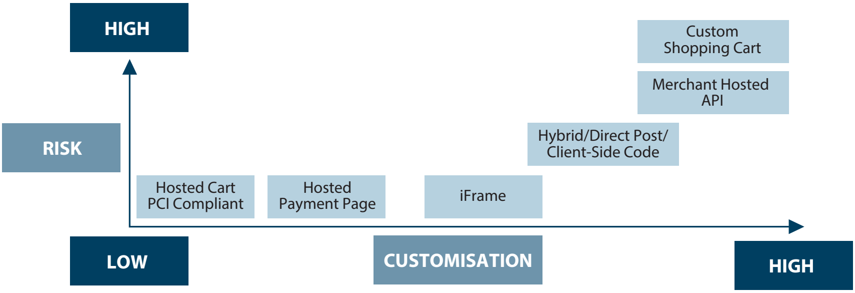
OPTIONS IN ORDER OF SOLUTION SECURITY

The diagram below outlines which payment gateway solutions minimise the risk using PCI DSS compliant service providers.

OPTION 1 Hosted Cart SAQ A	Is your website a PCI compliant fully Hosted Shopping Cart?	**If YES**, the responsibility for securing the cardholder data is with the hosted shopping cart service provider.
↓		**If NO**, go to option 2.
OPTION 2 Hosted Payment Page or iFrame SAQ A	Is your website's gateway integration using a hosted payment page or iFrame?	**If YES**, the responsibility for securing the cardholder data is with the payment gateway.
↓		**If NO**, go to option 3.
OPTION 3 Hybird Integration/ Direct Post SAQ A-EP	Is your website's gateway integration using a hybrid integration which posts transaction details to the gateway (also known as direct post)	**If YES**, the responsibility for securing the cardholder data is shared with the payment gateway and the merchant.
↓		**If NO**, the merchant is responsible for the security of the cardholder data and exposed to the likelihood of cardholder data being stolen.
OPTION 4 Merchant Hosted API SAQ D	Is your website's gateway integration using an API, where card processing is via your web server?	The responsibility for securing the cardholder data is with the merchant. The merchant must protect their website, web server and any connected systems. All of the PCI DSS requirements are the merchants responsibility and not the PCI compliant service provider.

Key
Lower Risk
Higher Risk

The risks associated with card payment products varies with customisation. Highly flexible systems also mean you need more investment into IT security controls. The table below demonstrates the scale of risk based on the customisation option you choose.



HOW TO MANAGE RECURRING PAYMENTS

Where there are instances of recurring payments, you can eliminate the need and risk of electronically storing cardholder data by using a tokenisation service.

Payment gateways provide tokenisation services either via their connectivity options or back office portal.

A token reference number is provided by the payment gateway and can be used to process payments instead of a card number.

A key rule should apply to eliminate or reduce any risk of data being compromised by fraudsters. If you don't need it don't store it.

PHONE PAYMENTS

When accepting payments over the phone ensure the card details are keyed directly into the payment gateway provided administration portal, also known as virtual terminal. This will eliminate any chance of card data being stored in your own environment.

STORING PROHIBITED PAYMENT CARD DATA

Protecting your customers as well as your business against misuse of credit and debit accounts is vital. Do not store prohibited cardholder data such as magnetic stripe data (track data), card verification value (CVV) and unencrypted account number.

PCI DSS COMPLIANCE DEFINITIONS

ADC – Account Data Compromise - An Account Data Compromise event (ADC) is unauthorised access to Payment Card Data (cardholder data) that is held within your business environment in either electronic or physical form.

AOC – Attestation of Compliance – A declaration of the merchant's or service provider's compliance status with the Payment Card Industry Data Security Standard (PCI DSS) Requirements and Security Assessment Procedures.

Cardholder details – Includes the 16 digit card number, expiry date and the card verification value.

Compromise – The act or result of breaking; or compromise. For example, a fraudster managed to breach our electronically stored card data.

PA DSS – Payment Application Data Security Standard – Applies to software vendors and others who develop payment applications that store, process, or transmit cardholder data as part of authorisation or settlement, where these payment applications are sold, distributed, or licensed to third parties.

PCI DSS – Payment Card Industry Data Security Standards – These set out how the industry is expected to protect payment card data.

PCI SSC – Payment Card Industry Security Standards Council – The PCI DSS requirements are set by the PCI SSC whose founding members are: Visa, MasterCard, Discover, JCB and American Express.

Prohibited data – Includes the track 1 and 2 magnetic stripe and card verification value information.

QSA – Qualified Security Assessor – Accredited by the PCI SSC to conduct independent third party PCI DSS assessments.

SAQ – Self-Assessment Questionnaires – Are developed by the PCI Council for merchants to report on their PCI status. These questionnaires determine what security controls are required to protect the cardholder details via your payment channels.

SAQ A - Self-Assessment Questionnaire A is limited to 14 security requirements and is only applicable for commerce merchants who are using a PCI compliant Hosted Shopping Cart or a PCI Compliant Payment Gateway Hosted Page or iFrame.

SAQ A EP - Self-Assessment Questionnaire A-EP has 140 security requirements and is only applicable for commerce merchants who are using a Client Side Code implementation otherwise known as Direct Post or Transparent Re-Direct.

SAQ D - Self-Assessment Questionnaire D has 326 security requirements and is applicable for merchants who use an API to process and/or store card payments via their websites. This SAQ is also relevant for merchants with multiple payment channels.

Service Provider – Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS (Intrusion Detection System) and other services, as well as hosting providers and other entities. If an entity provides a service that involves only the provision of public network access – such as a telecommunications company providing just the communication link – the entity would not be considered a service provider for that service (although they may be considered a service provider for other services). For further information and more definitions visit www.pcisecuritystandards.org/pci_security/glossary

PCI DSS HELPFUL LINKS

PCI SSC

Third-Party Security Assurance
www.pcisecuritystandards.org/documents/ThirdPartySecurityAssurance_March2016_FINAL.pdf

PCI SSC Website
www.pcisecuritystandards.org

PCI SSC Documents Library
www.pcisecuritystandards.org/security_standards/documents.php?document=2.0

PCI SSC Approved QSAs
www.pcisecuritystandards.org/approved_companies_providers/qsa_companies.php

VISA REFERENCES

Visa Steps for Staying PCI DSS Compliant
www.visa.com.au/partner-with-us/pci-dss-compliance-information.html

MASTERCARD REFERENCES

MasterCard PCI 360 Education Program
arm.mastercard.com/pci-360/

MasterCard Site Data Protection and PCI - How to Determine Service Provider Level and Validation

AUSTRALIAN PAYMENTS NETWORK AUSPAYNET

www.auspaynet.com.au/

Australia and New Zealand Banking Group Limited (ANZ) ABN 11 005 357 522. Item No. 91844 09.2021 WZ110746