ezidebit®
A division of globalpayments

Your guide to the Payment Card Industry Data Security Standard (PCIDSS)

July 2018

Contents

Introduction

At Ezidebit we are committed to providing our merchants with every assistance in protecting their business from the growing threat of an Account Data Compromise (ADC). Criminals are using increasingly sophisticated techniques to obtain customer account information, therefore it is critical that merchants implement rigorous controls to minimise the risk of being the subject of an ADC.

The Payment Card Industry Data Security Standards (PCI DSS) is a set of comprehensive requirements for enhancing best practices for any entity that stores, processes and/or transmits cardholder data. As a merchant it is important that you understand these standards and implement controls to your business environment to avoid potential loss or media attention associated with ADC. It is also important that you ensure that any third party entity that stores, processes and/or transmits cardholder account data on your behalf is compliant to PCI DSS.

The PCI DSS was developed by the Payment Card Industry Security Standards Council (PCI SSC) and has been formalised into the Mastercard Site Data Protection (SDP) and Visa Account Information Security (AIS) programs. It is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organisations proactively protect customer account data.

The PCI DSS consists of six core principles, which are accompanied by 12 requirements. The PCI DSS applies to all merchants, however the scope of your assessment changes depending on what solution you use and how you operate your business. These requirements can be viewed on the following page.

What are the 12 key requirements of the PCI DSS?

PCI DATA SECURITY STANDARD	
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 cardholder data 4. Encrypt transmission of cardholder data and sensitive information across open 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 cardholder 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 system and processes
Maintain an information security policy	12. Maintain a policy that addresses information security

Protect your business

At Ezidebit we continue to hold the highest level of PCI DSS possible. However we urge our merchants to ensure they are aware of these standards to ensure you are protecting your business, outside of your direct transactions with Ezidebit.

Compliance to the PCI DSS greatly reduces the possibility of being the subject of an ADC, and in turn protects your business reputation and ensures you retain customer confidence in your brand.

What is an Account Data Compromise (ADC)?

An ADC is when a person or group gains unauthorised access to cardholder data that is held within your business environment in either electronic or physical form. It can be identified in a number of ways however it is usually detected as a common point of purchase before cards are used fraudulently elsewhere.

What are potential impacts of an ADC?

If you become the subject of an ADC you risk financial penalties, the suspension or termination of your merchant facility, damage to your brand and reputation and having to undertake additional ongoing audit tasks.

There have been, and continue to be, many examples of ADC events worldwide and they have been experienced by all types of business, small and large. It is important to recognise that criminals do not target any particular type of business - if there is an identified weakness and they can exploit it, they will.

What is a Vulnerability Scan?

As a merchant of Ezidebit we want to ensure that you are always aware of risks to your business. We recommend that you complete regular vulnerability scans, especially when selling good or services via a website.

A vulnerability scan ensures that your systems are protected from external threats such as unauthorised access, hacking or malicious viruses. The scanning tools will test all of your network equipment, host and applications for known vulnerabilities. Scans are intended to be non-intrusive, and must be conducted by an Approved Scanning Vendor (ASV). A vulnerability scan would not ordinarily be required for a merchant using a stand-alone EFTPOS terminal.

Regular quarterly scans are necessary to ensure that your systems continue to to afford adequate levels of protection.

A current list of Approved Scanning Vendors (ASV) can be located on the PCI SSC website.

What are the requirements for Payment Applications?

If you implement any 'off the shelf' software applications, you must ensure that they are compliant to the Payment Application Data Security Standards (PA DSS). The PA DSS was developed by the PCI SSC to ensure that software vendors and others who develop payment applications that store, process and/or transmits cardholder data allow the environment in which it is implemented to be compliant to PCI DSS. By using Ezidebit, you can ensure that your data is stored, processed and transmitted under the requirements of these security standards.

Any payment application which is developed in house or heavily customised will be included in the scope of either the merchant's or the service provider's PCI DSS requirements and does not need to be compliant to the PA DSS.

What should I do in the event of a Data Compromise?

Immediately notify Ezidebit via our Client Support Team by contacting support@ezidebit.com.au or calling 1300 763 256. Within the first 24 hours, take action to prevent further loss of data.

For Further Information

Call: 1300 763 256
Visit: www.ezidebit.com
Email: support@ezidebit.com.au

ACN 096 902 813
AFS License 315388