A Merchants Guide to the

Payment Card Industry Data Security Standard (PCI DSS)

Elavon

secured BY ELAVON

Contents

Elavon

01

The Threat of Card Data Breaches

A single credit card is worth $0.50-$100 on the black market* which is why large databases or unsecure small businesses are a prime target for hackers

In 2016, 40% of information lost in data breaches was Personal Financial Information, including credit or debit card details or banking financial records.*

*Symantec Internet Security Threat Report, 2017

Hackers want your cardholder data. A thief can then impersonate the cardholder, use the card and steal the cardholder's identity.

The breach or theft like this affects the entire payment card ecosystem. Customers can lose trust in merchants or financial institutions, credit can be negatively affected, as well as potentially experiencing:

- Loss in sales and reputation
- Fraud losses
- Legal costs, settlements and judgments
- Fines and penalties
- Termination of ability to accept payment cards
- Lost jobs (Chief Information Security Officer, Chief Executive Officer and dependent professional positions)
- Going out of business

Elavon

02

A Bit of Background to Payment Security

To address this problem, Visa, Mastercard, JCB, Amex and Discover created the Payment Card Industry Data Security Standard (“PCI DSS”).

This standard recommends best practice methods in which merchants must manage, transmit, store and process card data.

Merchants must adhere to these standards and demonstrate that they are providing adequate security to keep customer card data safe, or face severe fines in the event of a data breach.

Elavon

03

What is PCI DSS?

The PCI Security Standards are a set of technical and operational requirements issued by the PCI Security Standards Council (PCI SSC) to protect cardholder data.

The standards apply to all merchants that store, process or transmit cardholder data – including those responsible for software development of applications and manufacturers of devices used in card payment transactions.

The PCI SCC is responsible for maintaining the Standard, while its compliance is enforced by the founding members of the Council; American Express, Discover Financial Services, JCB, MasterCard and Visa Inc.

If you accept or process payment cards, the PCI DSS applies to you.

Elavon

04

The 12 Requirements

PCI DSS applies to all the technical and operational system components that include or are connected to cardholder data. This means your instore card payment terminals, till, your networks, payment processes, and if you sell online, your local area and wide area network, phone lines and gateway, are all in scope for the standard. There are 12 requirements that need to be met:

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder 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 across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 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 systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

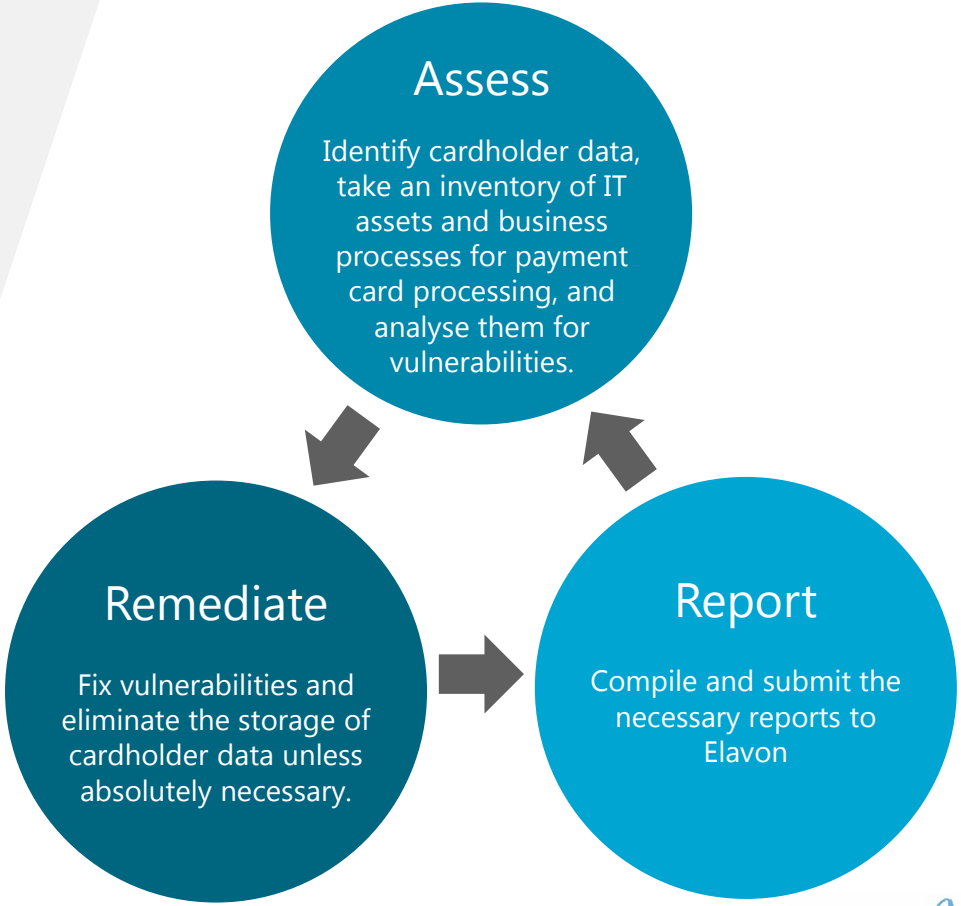
Elavon

05

A Continuous Process

PCI DSS aims to reduce credit card fraud by securing cardholder data through a 360° approach to security.

It also needs to be a continuous process, not an annual check, so cardholder data is being constantly monitored. The Standard is enforced using the controls specified within it:



Elavon

06

Your ‘Level’ and Validation Needs

Your business will fall into one of four merchants levels based on Visa or MasterCard transaction volumes over a 12-month period. The volume of transactions you process indicates what reporting is needed.

Level	Criteria	Validation
Level 1	Over 6 million Visa or MasterCard transactions processed per year.	Annual on-site review by a Qualified Security Assessor and a passing network scan by an approved scanning vendor (ASV) if applicable.
Level 2	1 million to 6 million Visa or MasterCard transactions processed per year.	Annual Completion of a Self-Assessment Questionnaire (SAQ) and a passing network scan with an ASV scan (if applicable).
Level 3	20,000 to 1 million Visa or MasterCard e-commerce transactions processed per year.	Annual completion of an SAQ and a network scan with a passing ASV scan (if applicable)
Level 4	Less than 1 million Visa of MasterCard transactions processed annually and under 20,000 e-commerce.	Annual completion of an SAQ and a network scan with a passing ASV scan.

Elavon

07

Assisting all Levels with PCI DSS

Whatever your level or size of business, or whether you are new to us as your Acquirer, Gateway Provider, Processor or new to accepting card payments, as a validated and listed PCI DSS service provider, we can assist you with your PCI DSS compliance in the following ways:

Track and monitor PCI DSS compliance programmes

Level 1-4 customers - as an acquirer, we need to ensure that you attest to and maintain PCI DSS compliance so we can accurately report this to the Card Schemes

Customer and Colleague Support - we offer personal consultancy to our corporate customers, working together to understand your business and individual PCI DSS compliance plans. For our small to medium enterprise customers, we offer a dedicated self-service compliance portal to complete their PCI DSS validation certificate.

Industry and Expert Knowledge – You will have access to a large pool of security talent and PCI Qualified Security Assessors and experts who keep up to date with the latest industry payment trends.

Elavon

08

Who does what for PCI DSS?

The **PCI SSC** is the governing body who writes and maintains the PCI DSS

As a **merchant**, you only have to submit one compliant Report on Compliance (ROC) or Self Assessment Questionnaire (SAQ) yearly to your acquirer(s), but must always maintain PCI DSS compliance.

Acquirers must notify their merchant customers about PCI DSS and their responsibilities. They also gather PCI DSS status information from merchants and report this to Card Schemes.

Card Schemes are responsible for programmes that merchants comply with. They receive card data directly from the acquirer, not the merchants.

Qualified Security Assessors (QSA) help Level 1 and 2 merchants reach full PCI DSS compliance to complete their SAQ by providing technical guidance. They can also create a ROC to confirm the merchant's compliance status.

Approved Scanning Vendors (ASV) conducts PCI Security Scans over the internet which help identify vulnerabilities of web sites, applications and information technology (IT) infrastructures.

Elavon

09

The General Data Protection Regulation (GDPR)

Information on GDPR:
http://ec.europa.eu/justice/data-protection/index_en.htm

The General Data Protection Regulation (GDPR) became law in all EU countries in May 2018. So whatever its size, if your business trades with customers within the EU or you have parts of your business located within the EU then you'll be subject to the GDPR.

PCI DSS can help provide the framework to assist in compliance of GDPR. Where PCI DSS is concerned with cardholder data, GDPR regulates all EU personal data.

If you're not yet GDPR Compliant, bear in mind that a data breach or failure to report qualifying incident within 72 hours, is liable to fines of up to £20m or 4% of your turnover (whichever is greater). If cardholder data is involved in the breach, additional fines from the PCI Council may also be applied.

Elavon

10

Providing a Framework for GDPR

Replacing one word within the 12 main requirements for PCI DSS will provide a logical structure to approach GDPR compliance

Goals	Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect **PERSONAL** data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored **PERSONAL** data 4. Encrypt transmission of **PERSONAL** data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to **PERSONAL** data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to **PERSONAL** data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and **PERSONAL** data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Elavon

11

Next Steps

It is your responsibility to become PCI DSS compliant but it's ours to support you where we can.

Whether you are fully compliant to the PCI DSS, working towards compliance, or even if you have never heard of the PCI Standards before, we can help you through the next steps.

What do I need as a merchant?	Next step Levels 1-3	Next step Level 4
"I have never heard of PCI DSS compliance and I am not aware of my responsibilities."	Please contact your Elavon Payment Data Security Consultant who will talk you through the process.	Please contact your Elavon Sales representative or email: elavonpci@elavon.com
"I am/we are working towards PCI DSS compliance"	Please forward evidence of your progress to your Elavon Payment Data Security Consultant for review.	Logon to your Secured by Elavon dedicated portal and update your details to reflect your current status.
"My business is fully PCI DSS compliant"	Please forward evidence of your compliance status that meets the Level validation requirements to your Elavon Payment Data Security Consultant for review.	Upload your Attestation of Compliance to the Secured by Elavon portal

Elavon

Any Questions?

Please contact us for further information on PCI DSS compliance and data security:

Level 3-4 Businesses

UK
0345 850 0195
elavonpci@elavon.com
elavon.co.uk/security

Ireland
1850 202 120
elavonpci@elavon.com
elavon.ie/security

Level 1-2 Corporates

UK
0345 850 0195
PCIEurope@elavon.com

Ireland
1850 202 120
PCIEurope@elavon.com

Report an Incident: ADCqueries-EU@elavon.com
UK: 01923 651 622
IRE: 0402 25 322