A Guide to Data Security

Elavon

secured
BY ELAVON

Contents

Elavon

01

Card data breaches are real

A single credit card is worth up to $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

Reports of data breaches in the media are on the rise. Cardholder data is extremely valuable and hackers are capitalising on this demand.

The growth in identity theft and thieves impersonating cardholders means businesses need to be more vigilant in protecting their business.

A data breach means a business could suffer:

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

Elavon

02

What is the Payment Security Standard?

The Card Brands, namely; Visa, Mastercard, JCB, Amex and Discover) developed the Payment Card Industry Data Security Standard (PCI DSS) which recommends best practice methods for card data security.

The standard applies to all businesses wherever they are, who store, process or transmit cardholder data.

PCI DSS can also help provide a framework to help businesses comply with data security requirements within the General Data Protection Regulation (GDPR), the new EU directive. The PCI DSS is concerned with cardholder data, whereas the GDPR regulates all personal data.

Businesses must be compliant with the standard or face severe fees and fines from Card Brands and Data Protection authorities in the event of a data breach.

Elavon

03

How do I adhere to this standard?

PCI DSS applies to all the technical and operational system components that process, store or transmit cardholder data.

This means your instore card payment terminals, tills, 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.

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

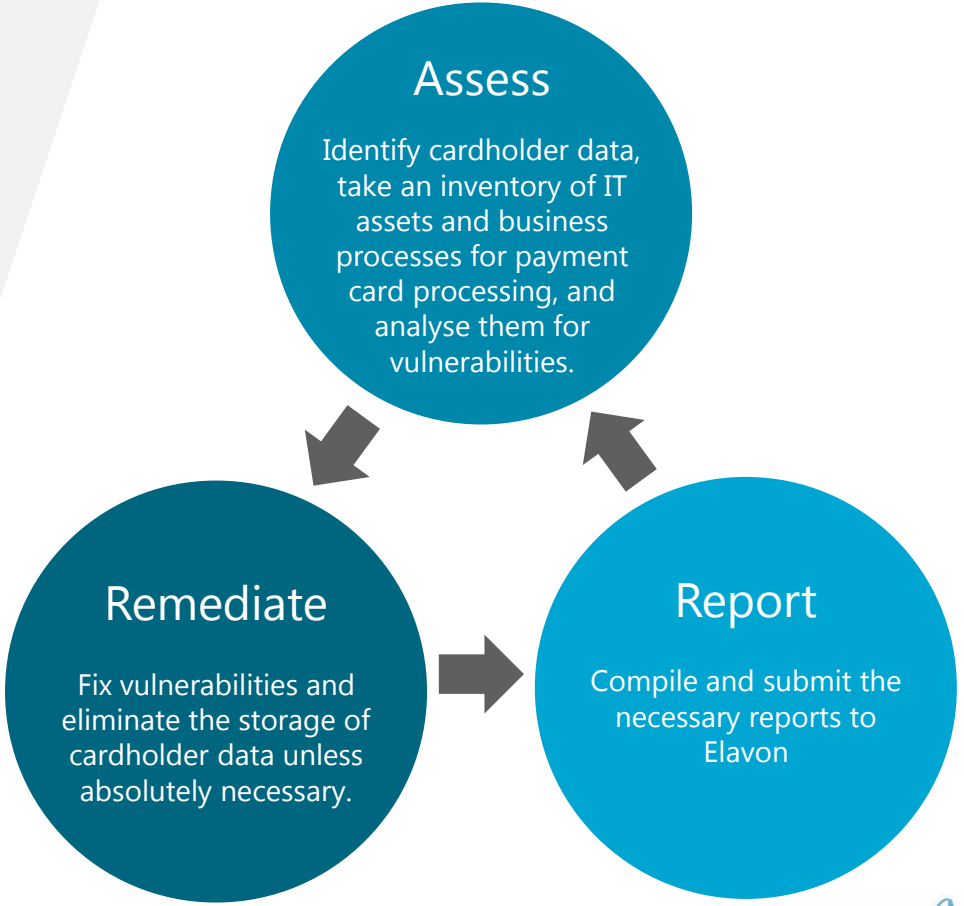
Elavon

04

How do I maintain PCI DSS compliance?

PCI DSS aims to reduce card fraud by ensuring that cardholder data is protected through a 360º approach to security.

Payment Security needs to be a continuous process, not just an annual check.



Elavon

05

What do I need to do for my business set up?

Your business will fall into one of four levels based on the number of Visa or Mastercard transactions processed over a 12 month period.

The volume of transactions you process indicates what level your business is and what validation is needed.

Level	Criteria	Validation
1	Any merchant processing over 6 million Visa or Mastercard transactions per year, has suffered a data breach, or identified as Level 1 by another card brand.	Annual on-site review by a Qualified Security Assessor and a passing network scan by an approved scanning vendor (ASV) if applicable.
2	Any merchant processing 1 million to 6 million Visa or Mastercard transactions per year.	Annual Completion of a Self-Assessment Questionnaire (SAQ) and a passing network scan with an ASV scan (if applicable).
3	Any eCommerce merchant processing 20,000 to 1 million Visa or Mastercard eCommerce transactions per year.	Annual completion of an SAQ and a network scan with a passing ASV scan (if applicable)
4	Any merchant processing less than 20,000 eCommerce transactions per year and all other merchants processing up to 1 million transactions per year, regardless of acceptance channel.	Annual completion of an SAQ and a network scan with a passing ASV scan.

Elavon

06

Here to protect

Whatever your level, complexity or size of business or wherever you are on your payment security journey, Elavon and it's trusted partners can assist you.

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. Our small to medium enterprise customers, can choose from a managed service or self service offering using our compliance portal to complete your PCI DSS validation

Industry and Expert Knowledge – You will have access to a large pool of security talent and PCI Qualified Security Assessors as well as data security experts who can support you in your payment card security needs

Elavon

07

Who's who in the Payment Card Industry?

The Payment Card Industry Security Standards Council (PCI SSC) is the governing body who writes and maintains the PCI DSS

You are required to submit a Report on Compliance (ROC) or Self Assessment Questionnaire (SAQ) yearly to your acquirer(s).

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

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

Qualified Security Assessors (QSA) help (customers reach PCI DSS compliance, can assist in SAQ completion by providing technical guidance. They will also help scope, audit and produce a Report on Compliance to confirm your compliance status.

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

Elavon

08

PCI DSS as a framework for the GDPR Data Security

All businesses that trade within the EU or have parts of your business located within the EU are subject to the GDPR.

Failure to demonstrate adequate security controls and other GDPR infringements can mean that businesses will be liable for fines of up to £20m or 4% of turnover (whichever is greater).

PCI DSS is a logical structure to approach GDPR compliance for Data Security.

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

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

Elavon

09

Here to safeguard

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

Whether you are fully compliant with the PCI DSS, are working towards compliance, or even if you have never heard of the PCI DSS 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 assist you through the process. Email: PCIEurope@elavon.com	Please contact your Elavon Sales representative or email: helpdesk@elavonsecuritymanager.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. Email: PCIEurope@elavon.com	Logon to your Secured by Elavon dedicated portal and update your details to reflect your current status www.elavonsecuritymanager.com
"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. Email: PCIEurope@elavon.com	Upload your Attestation of Compliance to the Secured by Elavon portal www.elavonsecuritymanager.com

Elavon

Here to safeguard

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

Level 4 Businesses

UK
0330 808 3301
helpdesk@elavonsecuritymanager.com
elavon.co.uk/security

Ireland
Ireland
1850 887 077
helpdesk@elavonsecuritymanager.com
elavon.ie/security

Level 1-3 Corporates

UK
PCIEurope@elavon.com

Ireland
PCIEurope@elavon.com

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