Payment security

(Please retain for your own records)

Important: Please read carefully **– you will need to take action.**

The Payment Card Industry Data Security Standard (PCI DSS) applies to all businesses that process, store or transmit payment cardholder data. It's a global standard published by the PCI Security Standards Council (PCI SSC) to maintain and enforce industry best practice for data security.

In essence, the PCI DSS is about preventing the card payment information held by you, or your third parties, from being used fraudulently. In the event that your customers card details are stolen, you may lose their trust to keep their information secure, which could damage your reputation. There can also be significant costs to your business, and you may lose the ability to take card payments through Barclaycard.

What could happen if you are not PCI DSS compliant?

If customer cardholder data which you or your third parties have handled is compromised, stolen or used fraudulently, this could be classed as Account Data Compromise (ADC) and you could be liable for:

- substantial financial penalties
- potentially high costs for forensic investigations which may involve scientific methods or skills to retrospectively determine what exactly happened in the past, issuer losses and business recovery

It is important that you let us know if you think you have lost payment card information so that we can help you through the investigation process. You can do this by calling us on 0800 161 5343*.

PCI Reporting Exemption Programme

If the information you have provided in your application has qualified you for our PCI Reporting Exemption Programme, it means that; -

- You are using a terminal(s) to take payments from customers in a face-to-face environment that is approved and accredited by Barclaycard Payments
- You are taking in a minimum of 95% of your annual transaction volume with the Card Present (CP)
- No more than 5% of your annual transactional volume is taken via Mail Order Telephone Order (MOTO) being keyed into the terminal
- Your business is either not in the process of undergoing a data breach or has reported a data breach within the last 12 months

Under the PCI Reporting Exemption, it is important to note that:

- Your business is still required to achieve and maintain compliance with the PCI DSS in accordance with your Merchant Acquiring Terms & Conditions– Barclaycard Payments will not however, require evidence of compliance, whilst you remain eligible for the reporting exemption
- Your business is required to establish and annually test an Incident Response Plan (IRP) in accordance with PCI DSS requirements – a template of an IRP can be downloaded for your use here https://www.barclaycard.co.uk/business/help-and-support/accepting-payments/taking-payments/resources This is an important document that should be completed and kept as part of your records
- Changes to the percentage of CP transactions are monitored bi-annually and should your business be identified as no longer qualifying for the exemption we'll let you know what actions you need to take to report your PCI Compliance to us.

More information on next page...

- If you are exempt from reporting your PCI compliance to us, you could still benefit from using our PCI reporting service (Data Security Manager) to document your PCI compliance for your records. Please contact us on 0800 161 5343 to let us know and we'll advise you further on how you can do this
- If you have decided to report your compliance to us instead of being included in the reporting exemption and later decide that you want to take advantage of the reporting exemption and still meet the eligibility criteria, then call us on 0800 161 5343 and we'll arrange this for you.

How Barclaycard can help

- Barclaycard offer two services to manage PCI DSS compliance reporting; the basic self-service package called Data Security Manager (DSM) or the premier 'handheld' service package called Proactive Security Service (PSS).
- We will let you know within 6 weeks of your account opening if you need to report your compliance to the PCI DSS. Should you need to report your compliance, you will be assigned an account on DSM and receive user credentials by post.
- DSM access is charged at £4.80 +VAT per month, per level at which you attest your compliance to the PCI DSS. Your level will be shown on your welcome letter. This fee will not apply if you have selected a Pay As You Go package.
- A 90 day grace period is in place from the date our Data Security Manager account is opened, to enable you to log- in to DSM, register, complete your profile and then the assigned Self-Assessment Questionnaire (SAQ), finally attesting your compliance at the end of the process. This must be repeated at a minimum every 12 months.
- If at 90 calendar days after being set up on DSM you have not reported your compliance via the DSM portal, as you will be non-compliant with the PCI DSS you'll be automatically upgraded to the PSS hand-held service, at a cost of £15 +VAT per outlet per month. An agent will contact you to guide you through all that needs to be done to achieve compliance every year.
- It is possible to opt out of this service if your preference is to remain on DSM. To opt out, call our Data Security Manager (DSM) help desk on 0800 015 9518* (+353 151 35150 for Ireland). Lines are open Monday – Friday from 8am to 8pm, and from 9am to 12 noon on Saturdays.
- If you choose not to use the PCI compliance services offered by Barclaycard you will still have an account on DSM which you'll need to use to upload your Attestation of Compliance (AOC) or your Self-Assessment Questionnaire to evidence your compliance status to us. If as part of your compliance validation, you are required to run quarterly vulnerability scans, they must be conducted by an Approved Scan Vendor (ASV) listed with the PCI Security Standards Council. The purpose of the scan is to conduct external vulnerability review of services to comply with PCI DSS requirements. You must upload the technical report demonstrating a pass status to the portal each quarter. If you are using an alternative PCI assessor and upload your AOC and SAQ documents there will be no charge for portal access.

Please note that any changes registered on or after the 16th of the month in relation to your choice of service (i.e. DSM, PSS) will not be reflected in your fees and charges until the following statement month. For more information on PCI DSS compliance requirements, please refer to 'Further help and industry resources' section at the end of this document.

More information on next page...

What do I need to do?

You'll receive your DSM username and password by post. Once received, you should log in to DSM at **barclaycard.co.uk/dsm** and follow the step-by-step process presented to you online, right through to attestation of compliance.

Further help and industry resources

If you want to find out more before you have access to Barclaycard Data Security Manager, you can find more information about Payment Security at **barclaycard.co.uk/pcidss**

You can reach the Data Security Manager helpdesk at **0800 015 9518** 8am to 8pm, Monday to Friday and 9am to midday on Saturday.

You can reach the Proactive Security Service team on **0330 058 3940*** 8am to 8pm, Monday to Friday and 9am to midday on Saturday.

Barclaycard PCI DSS compliance: Helping your business to stay safe: **www.barclaycard.co.uk/pcidss**

For more information about the PCI DSS, please visit the Payment Card Industry Security Standards Council (PCI SSC) website at: **www.pcisecuritystandards.org/**

Visa Europe downloads & resources:
ww.visaeurope.com/en/businesses__retailers/payment_security/downloads__resources.aspx

Visit Mastercard's website for compliant Payment Service Providers at:
www.mastercard.com/us/company/en/whatwedo/complaint_providers.html

Mastercard's Site Data Protection and PCI (SDP) programme:
www.mastercard.com/us/company/en/whatwedo/site_data_protection.html

Mastercard Merchant Education Programme:**www.mastercard.com/pci360**

Financial fraud issues and fraud prevention advice: **www.financialfraudaction.org.uk/**

OWASP guide to handling e-commerce: **www.owasp.org/index.php/Handling_E-Commerce_Payments**

*Calls to 03 numbers use free plan minutes if available; otherwise they cost the same as calls to 01/02 prefix numbers. Please check with your service provider.

Calls to 0800 numbers are free from UK landlines and personal mobiles, otherwise call charges may apply. International calls will be charged at a higher rate.

Calls may be monitored or recorded in order to maintain high levels of security and quality of service.

JUNE 2023