Is your customer data safe?

Every time your customers pay you by card, they're trusting you with their personal and financial information. But with the ever-increasing risk of fraud, are you doing what's needed to keep their cardholder data secure?

The Payment Card Industry Data Security Standard, or PCI DSS, was put in place to make sure that all payment card data is processed and stored securely. All merchants who accept payments by card must meet the standard.

What exactly is the PCI DSS?

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), which was founded by Visa, Mastercard, American Express, Discover Financial Services and JCB International. Its aim is to keep and enforce industry best practice for data security.

The PCI DSS isn't a 'standard for standard's sake'. It's a collection of good practices that any business should have in place.

In short, the PCI DSS aims to stop the card payment information that you or your third parties hold from being used by criminals. Because, **if your payment card data is stolen, the impact can be quick and costly.**

If your customers feel they can no longer trust you to keep their information safe, your reputation and your profits will suffer. If your data is stolen, you may also have to pay big financial penalties and your business may no longer be able to take card payments.

For the best and most up to date information on the PCI DSS, please take a look at the PCI SSC website: pcisecuritystandards.org

Does the PCI DSS apply to me?

The PCI DSS applies to any business that stores, processes or transmits cardholder data. It applies if you store and process cardholder information manually or electronically.

For instance, you could be storing your cardholder data in a way that the security standard doesn't allow (maybe you have poor passwords or use insecure websites). It's important that you have the best security for all the data you save on your systems.

As the company that enables you to take card payments, we are also required to track and confirm that you're meeting the requirements of the PCI DSS and report this to the card companies. That's why we put in your Merchant Agreement that you have to meet the standard – also known as being 'PCI DSS compliant'.

What do I have to do to meet the PCI DSS?

As a PCI DSS level 3 or 4 customer, you'll need to fill in a Self-Assessment Questionnaire (SAQ) and Attestation of Compliance (AOC). In addition, depending on how you process payments, you may have to carry out (and pass) network scans every three months. These must be set up by an Approved Scanning Vendor (ASV).

How can Barclaycard help me report my PCI DSS status?

We know your business is important to you – it's important to us too. That's why we want to help you strengthen your data security and keep meeting the required standard every year.

So, we have two services which you can use:

- our premium, 'hand-held' package, Proactive Security Service (PSS)
- our self-serve portal, Data Security Manager (DSM)*

How our Proactive Security Service (PSS) can help you

PSS gives you a dedicated point of contact to guide you through meeting the standard with the PCI DSS every year. They'll help profile your business to make sure you fill in the correct SAQ. And they'll remind you every time you need to take action to keep meeting the PCI DSS.

When you speak to your PSS team, they'll see if they can spot any problems with the way you're storing your cardholder data. They'll then tell you the steps you need to take to improve things, so that you meet the PCI DSS as quickly as possible.

The service is designed to help with all the tasks you need to do in order to meet the requirements of the PCI DSS every year. So, it can save both time and effort.

The service includes:

- **Compliance management dashboard:** use our mobile app to keep up to date with your PCI DSS status for all your registered merchant accounts
- **Quarterly vulnerability scans by an Approved Scanning Vendor (ASV):** scan your device, network and website to look for known security problems in line with the requirements of the PCI DSS
- **Vulnerability management:** scan your device(s) to look for known security problems that criminals could use
- **Card data discovery:** find out if you have any unencrypted card data on your device
- **Network discovery:** check to see what visible devices are using your internet connection
- **Anti-virus:** detect and remove known viruses and other dangerous software on your computer
- **Threat containment:** automatically weed out unknown, dangerous files to stop them causing harm

All the security tools are available for you to download at no extra cost.

What software is required to run the cybersecurity tools included with this service?

You must have an operating system that's currently supported by Microsoft (i.e. Windows), Apple (i.e. Mac OS) or Google (i.e. Android mobile). Please call +44 (0)330 058 3940** if you want to check with us.

You can also do it yourself with Data Security Manager

Data Security Manager (DSM) is our online portal which lets PCI level 3 and 4 customers meet the standard and report it to the PCI DSS every 12 months. If necessary, we can also help you get Approved Scanning Vendor (ASV) scans every three months.

When a new customer opens an account to accept card payments with Barclaycard, we also automatically open an account on DSM too. This lets you start reporting your status with the PCI DSS as quickly as possible.

We'll send you your username and password so you can get started and log in to DSM. To register, just answer a few questions and then fill out a profile of your business. This will allow the portal to give you the relevant Self-Assessment Questionnaire. You'll then be told if you're meeting the standard or need to take action.

You'll have 90 days from the date we open your account on DSM to finish the online process and show you're meeting the requirements of the PCI DSS. If you don't meet the standard after 90 days, you'll be automatically upgraded to our Proactive Security Service, so we can provide extra help to guide you through the tasks you need to do.

We'll write to you at least 60 days before this to remind you what you need to do and by when.

How do the two services compare?

Proactive Security Service	Data Security Manager
• We'll complete the self-assessment process with you to give you the best chance of meeting the PCI DSS first time • Get advice and guidance if you need to improve your data security • Get a suite of cybersecurity tools, at no extra cost, to improve your data security and help meet the requirements of the PCI DSS • Get reminders when you have tasks to do to keep your status with the PCI DSS • Get a dedicated point of contact, supported by a service telephone line and specialist team	• You'll complete the self-assessment process using the portal • Get access to Approved Scanning Vendor (ASV) scans if you need them for your business • Get helpdesk support by online live chat or on the telephone • Get email reminders to prompt you to take action when needed

How much will the service cost me?

Proactive Security Service	Data Security Manager
£15/€17 + VAT per Associated Outlet,[1] per month[3]	£4.80/€5.50 + VAT per Attestation Point,[2] per month

If you don't pay your bills in UK pounds, we'll convert the fees into your usual currency.

Do I have to join Barclaycard Proactive Security Service or Data Security Manager?

The Merchant Agreement you signed with us states that you have to keep meeting the requirements of the PCI DSS. This is so that we all fulfil our duties to the Card Schemes. We've set up these two services to help you do just that.

What happens if you meet the standard using PSS, but then choose to leave the service to use DSM instead?

You will immediately be told that you're not meeting the PCI DSS and will have to complete the steps shown on the portal.

Prefer to use the services of another PCI DSS assessor or Qualified Security Assessor (QSA)?

That's fine, but you'll still need an account on DSM to upload your current, valid Attestation of Compliance (AOC) or your completed Self-Assessment Questionnaire (SAQ). By doing it this way, you'll officially be reporting you're meeting the standard to us.

Please note we'll only accept you're meeting the requirement of the PCI DSS through DSM (self-assessment service or upload option) or PSS.

If you don't upload these documents, we can only assume you're not meeting the PCI DSS.

PCI Security Standards Council™
PARTICIPATING ORGANIZATION

[1]'Associated Outlet' refers to any outlet covered by your Attestation Point (sometimes the Associated Outlet may just be a single outlet).

[2]'Attestation Point' is the level at which you report meeting the PCI DSS. For instance, you may have one single attestation point to cover several outlets or one attestation point for each outlet.

[3]The monthly £15/€17 + VAT PSS fee assumes each Associated Outlet will require only one software deployment – either for a 'card present' environment or for ecommerce. If you require both for the same Associated Outlet, the monthly £15/€17 + VAT fee will be applied for each deployment.

Who can I contact for further information?

If you have an account on DSM and have any questions, go to barclaycard.co.uk/dsm to use our live chat feature or call our Data Security Helpdesk on 0800 015 9518[†] (Barclaycard Payments) and +353 (0)818 205270[Δ] (Barclaycard International Payments).

For questions about PSS, call our dedicated team on +44 (0)330 058 3940.[**]

We're here Monday to Friday from 8am to 8pm, and from 9am to 12 noon on Saturdays.

For general enquiries about payment security and the PCI DSS, please visit barclaycard.co.uk/business/help-and-support

Request this information in large print, Braille or audio. Just call 0800 161 5350 (Barclaycard Payments) or 1800 812 700 (Barclaycard International Payments).

[*]Minimum browser requirements: to access the DSM you'll need to have the latest versions of Internet Explorer, Firefox, Safari, Chrome or Adobe. If you don't have access to the internet, please call the Data Security Helpdesk on 0800 015 9518[†] (Barclaycard Payments) and +353 (0)818 205270[Δ] (Barclaycard International Payments).

[Δ]Calls to 0818 are charged at local call rates please check with your network provider charges may be higher from mobile network providers. [**]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 may be monitored or recorded in order to maintain high levels of security and quality of service.

9920150 PCILFT 0623

barclaycard | payments

Data protected

All the support you need to protect your customers from cardholder data theft