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 mandate that all payment card data is processed and stored securely. All merchants who accept payments by card are required to comply with 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 to maintain 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 would do well to have in place.

In essence, the PCI DSS is about preventing the card payment information held by you, or your third parties, from being used fraudulently because, **if your payment card data is breached, the fallout can be quick and costly**.

If your customers feel they can no longer trust you to keep their information secure, it damages your reputation and your bottom line. If the security of cardholder data is breached, there can also be costly financial penalties and your business may lose the ability to take card payments.

The best and most up-to-date source of information about the PCI DSS is the PCI SSC website **pcisecuritystandards.org**. Please take a look for yourself.

Does the PCI DSS apply to me?

The PCI DSS applies to any business that stores, processes or transmits cardholder data. It applies equally to manual and electronic methods of processing and storing cardholder information.

You may, for instance, be storing cardholder data in a way the security standard doesn't allow (for example, you may have poor password control or use insecure websites). It's important that all data saved on your systems has optimum security protection.

In addition, we, as your acquirer, and like all acquirers, are required to track and monitor your PCI DSS compliance status and report this to the Card Schemes. This is why the terms of your Merchant Agreement with us require you to be compliant with the Standard.

What do I have to do to become PCI DSS compliant?

As a PCI DSS level 3 or 4 customer, you'll need to report your compliance via a Self-Assessment Questionnaire (SAQ) and Attestation of Compliance (AOC). In addition, depending on how you process payments, you may have to complete (and pass) quarterly network scans, which have to be validated by an Approved Scanning Vendor (ASV).

How can Barclaycard help me to report compliance with the PCI DSS?

We know your business is important to you – it's important to us too, so we want to support you in strengthening your data security and ultimately maintaining and reporting a compliant status every year.

So we have two services available to you:

- our enhanced, 'hand held' package, Proactive Security Service (PSS), and;
- our self-serve portal, Data Security Manager (DSM)

How our Proactive Security Service can help you

PSS provides a dedicated point of contact to guide you through everything you'll need to report your compliance with the PCI DSS every year, from correctly profiling your business to ensure the relevant SAQ is completed, to reminding you every time you need to take action to maintain your compliant status.

If any weaknesses in your cardholder data environment are discovered during your conversations with the PSS team, you'll receive advice on the essential steps to remedy the situation quickly and efficiently in order to comply with the PCI DSS.

The service has been designed to save you time and effort and provide ongoing support with every PCI DSS related task, every year.

In addition, this service is packed with cybersecurity tools to help you strengthen your data environment and go further towards maintaining that all-important compliant status.

These include:

- **Vulnerability management:** scans your device and website to look for known security vulnerabilities that could be exploited
- **Quarterly vulnerability scans by an Approved Scanning Vendor (ASV):** scans your device and website to look for known security vulnerabilities in accordance with the requirements of the PCI DSS
- **Anti-virus:** helps detect and eliminate known viruses and other malicious software on your computer
- **Malware detection and prevention:** comprehensive protection of web applications from malware and other malicious attacks
- **Threat containment:** automatically isolates unknown, potentially damaging files to stop them from causing damage
- **Host intrusion prevention systems (HIPS):** helps to identify and stop unauthorised system changes
- **Endpoint firewall:** defends against inbound and outbound attacks on your computer
- **Card data discovery:** helps discover the presence of unencrypted primary account number card data on your device
- **SecureBox:** protects your point-of-sale application from malicious attacks
- **Managed web application firewall:** reduces risk of data security compromises of web application; a layer of defence in front of your website
- **Distributed denial of service (DDOS) protection:** helps defend against web applications being overloaded with traffic to ensure your website can stay operational
- **Content delivery network (CDN):** improves webpage loading times, performance and reliability

So you see, this really is a comprehensive package to help you beat the cyber criminals and meet your obligations to the Card Schemes – and it's all fully supported by our dedicated PSS team.

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

Your operating system must be a version currently supported by Microsoft (i.e. Windows), Apple (i.e. Mac OS) or Google (i.e. Android mobile). Please telephone **0330 058 3940**** in order to verify suitability.

Or maybe you'd rather self-serve using our Data Security Manager

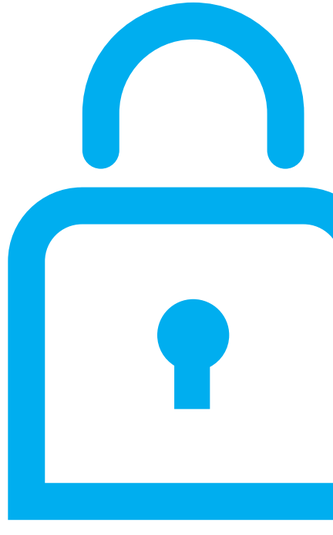
Barclaycard's DSM is our online portal which enables PCI level 3 and 4 customers to self-assess and attest to compliance with the PCI DSS every 12 months. Where relevant, quarterly approved scanning vendor (ASV) scans are also made available to you.

When a new customer opens their acquiring account with Barclaycard, an account on DSM is automatically arranged in order that an avenue for compliance reporting is quickly open to the customer.

You'll receive username and password information from us and then you can log in to DSM, register by answering a few questions and then complete a profile of your business. This will enable the portal to assign the relevant Self-Assessment Questionnaire for you to complete, from which you'll be advised if you're compliant or need to take action to become compliant.

You'll have 90 days from the date your account opens on DSM to complete the online process, ultimately attesting your compliance with the PCI DSS. After that time, if you fail to become compliant with the PCI DSS, you'll be automatically upgraded to the Proactive Security Service so we can provide additional support to aid you in all the stages of achieving compliance.

We'll write to you at least 60 days ahead of that deadline 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 optimise the likelihood of compliance with the PCI DSS first time • Advice and guidance where data security improvements are required • A suite of cybersecurity tools to enhance your data security, also supporting compliance with the PCI DSS • We'll remind you when PCI DSS related tasks are due to maintain your compliance • Dedicated point of contact, supported by a service telephone line and specialist team	• You'll complete the self-assessment process using the portal • Access to Approved Scanning Vendor (ASV) scans if applicable for your business • Help desk support available via online live chat feature or telephone • Email reminders prompt you to take action when needed

How much will the service cost me?

If you use our Proactive Security Service, every outlet will receive the enhanced security package as outlined above, which is why the fee applies to each of your Associated Outlets[1], rather than your overall Attestation Point.[2]

PSS could also prevent PCI DSS non-compliance charges being applied as you'll have 12 months to achieve a compliant status, which our team will then help you to maintain every year.

Proactive Security Service	Data Security Manager
£15 per Associated Outlet, per month[3]	£4.80 per Attestation Point, per month

[1]"Associated Outlet" refers to any outlet on whose behalf the Attestation Point is reporting (including where the Associated Outlet is a single outlet).

[2]"Attestation Point" refers to the level at which you report your compliance, i.e. one single attestation for a number of outlets or an individual attestation for each outlet.

[3]The monthly £15 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 fee will be applied for each deployment or currency equivalent, if you are not billed in sterling.

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

Under the terms of your Merchant Agreement with us, you've committed to maintain compliance with the PCI DSS, in order that we all fulfil our obligations to the Card Schemes. We've set up these two services to help you do just that.

If you achieve compliance through PSS, but then choose to leave the service to report compliance via DSM instead, you will immediately be deemed non-compliant with the PCI DSS until you complete the self-assessment and attestation process on the portal. This means that non-compliance charges may be applied if you don't complete this process straight away.

However, if you'd rather use the services of another PCI DSS assessor or Qualified Security Assessor (QSA), of course you can do so.

In this instance you'll still need an account on DSM, but you'd only use it to upload your current, valid Attestation of Compliance (AOC) or your completed Self-Assessment Questionnaire (SAQ).

By doing so you'll officially be reporting your compliance to us.

Please note we'll only acknowledge your compliance with the PCI DSS through DSM (self-assessment service or upload option) or PSS.

If you fail to upload this documentation, we can only assume you're non-compliant with the PCI DSS and therefore non-compliant charges will be applied.

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 **0844 811 0089.**†

For questions about PSS take a look at **barclaycard.co.uk/PSS** or call our dedicated team on **0330 058 3940.**††

Lines are open Monday – 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**

PCI Security Standards Council
PARTICIPATING ORGANIZATION

This information is also available in large print, Braille and audio format by calling 0800 161 5350

†Call charges apply. 0844 calls will cost up to 7p per minute plus your phone company's access charge (current at May 2018). Calls may be monitored or recorded in order to maintain high levels of security and quality of service.

††Calls to 03 numbers use free plan minutes if available; otherwise they cost the same as calls to 01/02 prefix numbers.

Calls to 0800 numbers are free from UK landlines and personal mobiles, otherwise call charges may apply. Please check with your service provider.

BCD000195840 PCILFT 0518

Data protected

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