Contents

What is PCI DSS?

What is PCI DSS, and who is it regulated by?

The Payment Card Industry Data Security Standard (PCI DSS) is a worldwide mandate from the PCI Security Standards Council (PCI SSC). The council consists of VISA, MasterCard, American Express, Discover and JCB, (the five major card schemes worldwide).

PCI DSS was established to help organisations processing credit and debit card payments to ensure controls are in place to prevent fraud. Business areas covered range from how business owners and employees handle payment cards to how systems are set up within a business. The PCI DSS standard applies to all organisations accepting, processing and or storing cardholder information from the card brands.

What is Barclaycard Data Security Manager?

Barclaycard Data Security Manager is a service that has been introduced to provide merchants with all the tools needed to record and maintain compliance with the PCI DSS.

What exactly is the PCI DSS standard about?

There are twelve requirements which are grouped under six categories:

Build and maintain a secure network

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor supplied defaults for system passwords and other security parameters

Protect cardholder data

3. Protect stored data (use encryption)
4. Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a vulnerability management program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement strong access control measures

7. Restrict access to 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 more information, please refer to the PCI Security Council's website: www.pcisecuritystandards.org

Compliance is not a one off exercise, businesses are expected to maintain compliance at all times and every year attest to their compliance.

Who needs to be compliant with PCI DSS?

Any organisation regardless of size or quantity of transactions accepting, storing, processing or transmitting payment card data by card brands.

This includes, banks, payment service providers, public sector organisations, retailers, utility providers, ecommerce, face to face and mail or telephone order merchant businesses.

Why do businesses need to comply?

PCI DSS was established to help organisations processing credit and debit card payments to ensure controls are in place to prevent fraud by reducing risk.

Business areas covered range from how business owners and employees handle payment cards to how systems are set up within a business. The PCI DSS standard applies to all organisations accepting, processing and or storing cardholder information from the card brands.

How much will it cost me?

A small fee applies for the Barclaycard Data Security Manager; please refer to the letter we sent to you for the amount.

What does the cost cover?

Expert PCI DSS help and support via our dedicated Data Security Helpdesk and an easy to follow online Self-Assessment tool.

Do I have to join Barclaycard Data Security Manager?

Yes. This forms part of the Merchant Agreement with Barclaycard for accepting card payments. All merchants need to be registered as PCI DSS compliant. Unfortunately our experience to date is that merchants who complete the Self-Assessment by themselves often misunderstand the questions and inadvertently believe they are compliant when they are not. We are seeing many more such merchants falling victim of data breaches and it is for this reason that we must insist that merchants use our service to either complete the SAQ online or upload an SAQ that a Qualified Security Assessor (QSA) has validated.

Why is Barclaycard putting so much pressure on me to be PCI DSS compliant?

As it is Barclaycard's duty to regularly report to VISA and MasterCard on the status of their merchants' PCI DSS compliance, we want to make sure that all our merchants are aware of their responsibilities.

It is the Card Schemes' prerogative to select merchants to investigate from the reports that Barclaycard submit, and to levy non-compliance fines as a result.

Over and above this, there are compromise fines and fraud costs associated with any breaches.

It is therefore Barclaycard's responsibility to warn all its merchants of these risks, so they can take appropriate action. In such cases, non-compliant merchants will be liable for these fines.

Merchant validation of compliance shows the merchant has taken all reasonable steps to protect the card holder data in their charge. Going through the compliance process also helps the merchant to improve their processes and work more securely.

Barclaycard are not unique in requiring their merchants to be PCI DSS compliant, all card acquirers have the same responsibility.

Are all PCI DSS requirements mandatory or can I leave some out as "nice to have"

The 12 PCI DSS requirements are mandatory.

However, depending on what methods are used to process payments i.e. telephone, face to face or on the internet and if the payment is processed by a third party, the merchant may exclude sections and this will be determined by the type of Self-Assessment Questionnaire (SAQ) being completed.

Barclaycard Data Security Manager is designed to determine the SAQ type appropriate to the business from the answers given in the Business Profile section.

If a merchant requires some help in prioritising their compliance work, Barclaycard have the following top tips to help with this:

- Do not treat PCI DSS as an IT project: it is a Change Programme and needs organisational commitment.
- Train staff at all levels (there will be various degrees of training).
- Understand how card payments are currently processed (people, process and technology).
- If you don't need cardholder information, don't keep it
- Embed an Information Security culture within your organisation early.
- There will be many quick wins derived by reviewing and changing business processes and historical practices that require little investment.
- Develop a gap analysis between current practices and what is necessary to become PCI DSS compliant: the gap analysis and Cardholder data flow mapping is the most important step.
- Reducing the scope of the cardholder environment (the smaller, the easier).
- Address vulnerabilities in the Card Not Present environment first (e-commerce and Mail Order/ Telephone Order).
- Outsource to compliant third parties where possible & (Barclaycard's e-PDQ has been compliant since 2007). Software as a Service (SaaS) is increasingly seen as a means of achieving compliance quicker.
- And if not possible, tie down third parties (contractually).
- Assess suitability/ Implement risk mitigation technologies (e.g. Verified by Visa, Secure Code, tokenisation, point-to-point encryption, etc.); these will also help reduce risk.
- If Compensating Controls are required ensure that all parties are engaged to agree the controls before implementation (merchant, QSA, acquirers)
- Work in partnership with your acquirer and your Qualified Security Assessor (QSA).

What is the Payment Application Data Security Standard (PA-DSS)?

The PA-DSS applies to any entity that has either developed software or has integrated payment applications for the purpose of storing, processing or transmitting cardholder data as part of the authorisation or settlement when these applications are sold, distributed or licensed to third parties. A full list of validated applications can be found on the https://www.pcisecuritystandards.org/

Who has to have an annual Formal Onsite Assessment?

The following types of businesses are required to have an annual formal onsite assessment:

- Any business accepting more than six million transactions per card scheme brand, per annum
- Payment Service Providers, processing over 300,000 transactions a year
- Most banks

What is a QSA? What does a Qualified Security Assessor do?

Qualified Security Assessors (QSA's) are information security consultants that have been trained and certified by the PCI Security Standards Council.

QSA's carry out on-site security assessments for organisations to verify their compliance with PCI DSS.

What is an ISA? What does an Internal Security Assessor do?

The Internal Security Assessor is where you elect a member of your staff to attend the ISA training course which is operated by the PCI Security standards Council. The course will be at your business' expense and your elected colleague will need to pass the course in order to be fully qualified. This is a recognised qualification and will then enable your elected member of staff to certify PCI DSS Compliance on behalf of your business. This is normally only relevant to larger organisations, acquiring banks and payment processors. An organisations' Internal Security Assessor facilitates the interaction with QSA's to enhance the quality, reliability and consistency of the organisations internal PCI DSS requirements. The ISA ensures the correct application of PCI DSS measures and controls are in place.

What are the different PCI levels and how are they decided?

A number of different risk levels have been identified by the card brands which have formed the basis of the various PCI levels.

PCI Level 1 and 2 businesses are required to carry out an onsite assessment, submitting a completed and signed Report on Compliance (RoC) to their acquirer. An onsite assessment is carried out by a Qualified Security Assessor (QSA) or a fully certified Internal Security Assessor (ISA).

PCI Level 3 and 4 businesses are required to complete a Self-Assessment Questionnaire (SAQ) and submit this to their acquirer. For the most part acquiring organisations provide a PCI DSS programme to facilitate this.

At any time we can change the PCI level of your business to level 1. Normally this would apply if your business has been hacked and subjected to a data breach where customer card data has been stolen.

PCI levels are set out by the card schemes and Barclaycard has summarised as follows:

Level	Type of business	Actions required for compliancy
1[1]	Any merchant processing over 6 million VISA or MasterCard transactions a year[2]	• PCI DSS compliance reporting managed by the Barclaycard Payment Security team. • Annual onsite security assessment by PCI SSC Accredited Qualified Security Assessor (QSA). • Quarterly network scan (certified by an Approved Scan Vendor) • Annual penetration testing • Implemented Security Policies
2	Any merchant processing 1 to 6 million VISA or MasterCard transactions a year	• PCI DSS compliance reporting managed by the Barclaycard Payment Security team. • Annual Self Assessment Questionnaire by a PCI SSC Accredited Internal Security Assessor (ISA) *or* an Annual onsite security assessment by PCI SSC Accredited Qualified Security Assessor[3] • Quarterly network scan (if in e-commerce) • Annual penetration testing • Implemented Security Policies
3	Any merchant processing 20,000 to 1 million VISA or MasterCard e-commerce transactions a year	• PCI DSS compliance is managed through Barclaycard's Data Security Manager (DSM) service. • Details of DSM will be sent to new customers no earlier than 4 months from account set-up, including details of a possible monthly charge for the Data Security Manager service. • Complete the online profile and follow up steps to complete your Self-assessment and compliance validation each year, or • In the DSM profile, upload a Self-assessment Questionnaire (SAQ) and attestation that has been validated by a Qualified Security Assessor (QSA) each year. • If you have any questions regarding PCI DSS compliance or Barclaycard Data Security Manager please call our Data Security Helpdesk on **0844 811 0089*** Monday to Friday 8am – 8pm and 9am – midday on Saturdays. • 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); this can be done using the Barclaycard Data Security Manager service. Or if you prefer, you can use an ASV listed with the PCI security standards organisation (see below for details). If you use another ASV you must upload the technical report demonstrating a pass status to the portal each quarter.
4	Any e-commerce only merchant processing fewer than 20,000 VISA or MasterCard transactions a year Non e-commerce merchants processing up to 1 million VISA or MasterCard transactions a year	

1 Compromised entities may be escalated at regional discretion

2 Where merchants operate in more than one country or region, if they meet level one criteria in any Visa country or region, they are considered a global Level one merchant. An exception may apply to global merchants if there is no common infrastructure and if Visa data is not aggregated across borders. In such cases merchants are validated according to regional levels.

3 With effect from 30th June 2012 any Level 2 merchant choosing to complete an annual Self Assessment Questionnaire (SAQ) must ensure that all staff engaged in the self-assessment attend PCI Security Standard Council (PCI SSC)-offered merchant training programmes and pass any associated PCI SSC accreditation program annually in order to continue the option of self-assessment for compliance validation.

Why do I need to do this?

If you take card payments from your customers you must do so securely in order to protect your customers' payment card information. The PCI DSS standard was developed by the card brands to ensure that businesses understand what securely means and follow guidelines to prevent fraud.

Not being PCI DSS compliant can be likened to getting into a car with no insurance. If you cause an accident you will be held liable and you will have to cover the cost of any damages out of your own pocket. PCI DSS works in a similar way, if you are compliant it can be likened to having a fully comprehensive cover, so the cost of damages is greatly reduced. However, if you are not compliant you will be liable for the full cost of a data breach where card data has been stolen. This will carry significant cost impact, a potential for reputational damage and loss of customer trust.

I did my PCI DSS compliance last year, why do I need to do this again?

You need to validate your compliance annually. Protecting your business is on ongoing challenge and ensuring that you comply with PCI DSS is ensuring you are taking steps in order to protect your business.

The purpose is to make sure that businesses comply at all times with a minimum standard in protecting themselves and their customer card data from payment card fraud.

The standard is also updated in line with changing market impacts, for example if you think about how technology has changed the methods in which debit and credit cards can be accepted. In addition the standard is also updated to ensure that new and emerging security threats are factored in.

Why do I have to do this, isn't my terminal secure?

Having a PCI validated point-of-sale solution certainly helps your annual PCI DSS assessment; however, it does not guarantee PCI DSS compliance. You have a responsibility to ensure that the relevant policies, procedures and controls are in place (and practiced by you and your staff) to minimise exposure and reduce the likelihood of a data breach. This program will take you through the steps needed to protect your business.

I outsource all my cardholder data functions via a third party service provider; do I still need to do this?

Outsourcing cardholder data functions to a third-party service provider does not exclude a company from PCI compliance. It may reduce the scope of your annual assessment and consequently reduce the amount of time and effort to validate compliance.

You need to make sure that your service provider(s) are PCI DSS compliant by checking listings on the Visa and MasterCard list or asking for proof i.e. a PCI DSS level 1 service provider certificate attested by a Qualified Security Assessor (QSA). It's important to check that the certificate covers the service you are using as some companies provide many products and services not all of which may be covered.

You also need to consider what you and or your staff do with your customer's card information. Are you securely destroying receipts? You also need to have a policy in place to ensure that everyone in your business is aware of any possible risk factors.

How often do I have to comply with PCI?

You must be compliant with PCI DSS at all times to ensure that you are taking adequate steps to protect your business. You are required to report, confirm and validate your compliance once a year. If you are required to complete scanning this must be done every three months to maintain your compliance.

I already completed and validated my compliance with another QSA, why do I need to do this?

You are still required to enrol and upload your documents in this programme, however you will not be asked to complete the Self-Assessment Questionnaire. You will be required to provide a copy of your Validation Certificate, your Attestation of Compliance and any scan results, which will have been issued to you by your QSA.

What do I have to do?

3 stages to complete on this portal to complete your PCI DSS

This portal was designed to make users PCI DSS journey as easy as possible.

There are three main stages that every business needs to complete. The first is to complete your online profile which helps us to understand what risk factors and questions are relevant. The next stage is to complete your security assessment, this is also known as a Self-Assessment Questionnaire (SAQ) which will involve a series of questions and in some cases scanning of the computer systems within your business. Once these two stages are complete you will then need to confirm and validate that all information provided is correct, officially referred to as Attestation of Compliance.

Business Profile

The purpose of building your business profile is to help us understand how your business is set up and what risk factors you may have. The profile is designed to ensure that you provide us with a comprehensive understanding of how your business is set up. From your profile we will understand what risk factors are specific to your business.

This ensures that we only present you with the security questions relevant to you.

What is a Self-Assessment Questionnaire (SAQ)

The Self-Assessment Questionnaire is used to help businesses demonstrate to the card schemes that they are compliant with the requirements of PCI DSS, or are at least working towards compliance.

The questionnaire was developed by the PCI Security Standards Council to allow businesses to self-assess so they do not need to undergo an onsite security assessment for their PCI compliance. The business profile on this portal was developed to help prepopulate answers as part of your security assessment, reducing the time you need to spend on your SAQ.

ASV Scanning

If you electronically transmit cardholder data or have a payment system connected to the internet you need to do quarterly scans, which must be performed by an Approved Scanning Vendor (ASV). Sysnet are the ASV provider for this programme.

There are a few reasons you may need to do ASV scanning every three months:

- If your payment terminal is connected via an internet cable
- If you host a payment page, transmit payment card data via an API link
- If you store credit and debit card electronically (even if only momentarily).

A clean passing ASV scan must be achieved and validated to every three months in order to achieve and maintain your compliance.

How do I verify my PCI DSS compliance?

If you need to do a Self-Assessment Questionnaire, the easiest method is to sign up to a PCI DSS programme, like this one. Once you have signed up to your PCI DSS programme you will be provided with log on credentials. You will be asked a series of questions about your business and based on your answers, you may then be presented with a set of tasks specific to your business.

Once you have completed the tasks assigned to you, you will be asked to confirm and validate that all of your answers are correct.

Will you tell me what I need to do and when?

We will get in touch with you by email when your PCI is due to expire so that you can be sure to complete your PCI DSS requirements when they are due, so please make sure that you provide us with a valid email address and correct contact name. You will also receive email reminders from us only as and when tasks are due or if certain areas aren't completed.

You may need to ensure that our email isn't being sent to your junk or spam folder. The best way to ensure that our emails are arriving correctly into your inbox is to whitelist our email address. How you do this will depend on your email service provider be it Outlook, Gmail, Yahoo etc.

Please add Notifications@barclaycarddatasecuritymanager.co.uk and pcidss@barclaycarddatasecuritymanager.co.uk to your safe senders list.

What is a Data Breach?

'A compromise occurs when cardholder information taken by your business to process a payment is obtained by an unauthorised person with the intent to commit fraud.'

What happens if I don't comply with PCI DSS?

Not being compliant with the PCI DSS can leave your business at risk of a breach (otherwise known as an Account Data Compromise) and breach related costs.

What happens if I suffer a data breach (lose customer card data)? **Cost implications and penalties.**

Breach related costs normally include card scheme fines, card replacement costs, reputational damage, customer confidence, lawsuits and audits. The exact cost depends on the damage caused, specifically the number of cards compromised so it can add up to a huge cost for any business.

In 2016 the scheme penalties for losing card information increased significantly here are a couple of examples:

Example one

Let's say a business loses card and CVV numbers for 46,706 Visa and 28,336 MasterCard customers. Under the old policy, the business would've paid just over £35,000 in penalties. With the new policy, they'll pay over £134,000. Here's how:

Type of cost	**Amount**	**What that means**
Visa penalty	£108,776.90	based on VISA cards impacted and business turnover capped at 5%
Visa management fee	£2,197.07	This is a new fixed penalty 3,000 Euro
MasterCard penalty	£0.00	There's no fee as less than 30,000 MasterCard accounts were affected
Forensic investigation cost	£12,000	That's based on the average cost of a full investigation
Post-breach compliance report signed by QSA	£12,000	Also based on average cost
Additional costs depending on business		
Total	**£134,973.97**	

Example two

Let's say a business loses 1,478 Visa card numbers and 1,478 MasterCard numbers. As there are less than 10,000 cards at risk, the Card Schemes agreed a scaled-down forensic investigation and to waive some penalties as long as:

- a PCI Forensic investigation (PFI light) investigation was completed in 40 days
- they made changes to their service provider
- and the investigator completed a Self-Assessment Questionnaire (SAQ) to confirm compliance was met

Under the old policy, they'd be charged £3,500. With the new policy, they'd be charged around £5,697. Here's how:

Type of cost	**Amount**	**What that means**
Visa penalty	£0.00	Waived because the PFI light conditions were met
Visa management fee	£2,197.07	This is a new fixed penalty 3,000 Euro

MasterCard penalty	£0.00	There's no fee as less than 30,000 MasterCard accounts were affected
Forensic investigation cost	£3,500.	That's a fixed cost for the investigation and report
Post-breach compliance report signed by QSA	£0.00	This wasn't needed, but the business did need to meet the above conditions
Additional costs depending on business		
Total	**£5,697.07**	

In addition customers may lose trust in your business and the loss of business caused by damage to your reputation can be difficult to put a figure on.

Formal onsite assessment requiring QSA

If your business has been subjected to a breach you will have to undergo a forensic investigation, which your business will be required to cover the cost of. Once the problem area has been found you will be required to secure this.

Following on from this your business will be flagged as a high risk business and will require ongoing QSA support until your acquiring organisation is satisfied that you have the correct controls in place keeping your customers card data safe and secure.

Having problems?

Are you sure that you have completed your business profile correctly

As you proceed through your profile make sure that you answer the questions correctly. For example, if you are being asked to complete scanning but you don't have internet connected equipment in your premises or an ecommerce website then you may have answered a question incorrectly.

You can re-profile at any time if you think you have made a mistake. If you are unsure or need help at any point you can use the live chat link, or call the help desk.

What is a network?

If you operate computers and equipment, including PC's, servers, firewalls, network devices, wireless access points, POS tills on your business premises this is what is referred to as your network.

If your business network is connected to the internet, and your payment terminal is on this network you need to ensure you are taking appropriate security precautions.

You will need to understand how your network is connected and interconnected. For some businesses you may need to engage the help of the IT specialist who may have set up your business network for you.

At each and every point that your network is externally connected you need a firewall. Additional firewalls are recommended specifically including a Demilitarised Zone (DMZ) to increase security. If you have a Demilitarised Zone then you will need to allow for a firewall at each of these points too.

You will also need to have a network diagram or sketch which illustrates how each and every piece of equipment is connected and interconnected.

What if I need more help?

You can always click on the Live chat button for clarity if at any time you are unsure of a question or need clarity around certain areas. Alternatively if you would prefer to speak with our help desk you can call 0844 811 0089.

You may also find some of the questions are very technical, especially if you have a network within your business, if this is the case you may need to get advice from your IT specialist to help you in certain areas.

How do I find my IP address?

If your terminal is connected via an internet cable you will need to identify the address of this on the internet.

The easiest way to do this is to unplug the cable from the back of your terminal and plug it into a laptop or computer. Go to your preferred browser and go to www.whatismyip.com this will give you a series of numbers and stops, this is the external facing IP address of your business.

Why am I not receiving emails from you?

To ensure that you receive emails from us, you may need to whitelist our email address to make sure they aren't going into your spam or junk mail. Each and every email service provider may have a different method for whitelisting of emails which you should be able to find in their help section.

Guide to ASV scanning

Why am I being asked to carry out scans?

If you electronically transmit cardholder data or have a payment system connected to the internet you need to do quarterly network vulnerability scans, which must be performed by an Approved Scanning Vendor (ASV). Sysnet is the ASV provider for this programme; however you can upload passing results from another provider if you want to.

There are a few reasons you may need to do ASV scanning every three months:

- If your payment terminal is connected via an internet cable
- If you host a payment page, transmit payment card data via an API link
- If you store credit and debit card electronically (even if only momentarily).

A clean ASV scan must be achieved and validated to every three months in order to achieve and maintain your scan compliance.

What is a network vulnerability scan or ASV scan?

A network vulnerability scan or ASV scan is like having a security guard walk around the perimeter of your business premises, checking if the doors and windows are locked and letting you know if anything has been left open so that you can lock up any possible entry points.

An ASV scan works just like a security guard. It is an automated, non-intrusive scan that assesses the security of your externally facing IP addresses and web applications from the internet. The scan will identify any vulnerabilities or gaps that may allow an unauthorised malicious hacker to gain access to your network and possibly steal your customer's card data.

How often do I need to run these scans?

Quarterly scanning is a requirement of PCI DSS, as set out by the card schemes (VISA, MasterCard, American Express, Discover and JCB).

Who carries out these scans?

These scans must be carried out by an Approved Scanning Vendor (ASV). These are scanning vendors approved by the Payment Card Industry Security Standards Council. Sysnet provide the ASV scanning requirement through this programme; however you can upload from another scan vendor if you want to.

What is an IP Address

An IP address is a series of numbers, separated by stops for example 111.111.111 which indicates an address or location on the internet.

It has a similar function in a way to a postcode for a physical address in that it identifies the specific location or address on the internet of a business network.

What is meant by a Domain?

For PCI DSS purposes, a domain is the url for your website. For example www.mywebsite.com or https://mywebsite.com

What are Load Balancers?

A load balancer can be on either a website or a router.

On a website, a load balancer will distribute the traffic to your website across multiple resources to ensure your customers can access your site if and when you have a surge in traffic.

For example, if you think about a website that sells tickets online to events. They may have a huge surge when the tickets are released and would need load balancers to ensure their website doesn't crash. This is something that you would have requested to have had built specially for your website to allow for very large traffic spikes.

You may also need to check with your website hosting provider if you have permission to scan.

Some routers have load balancers, to find out if your router has a load balancer you need to check the manufacturer's manual.

What happens if I fail a scan?

You will be provided with a report detailing out any vulnerable points in your network. You need to fix any problems as soon as you can to protect your organisation against hackers.

If you need help working out how to fix these issues, you can get in touch with our helpdesk through the Live chat function or by calling 0844 811 0089

My account

Email

Always ensure that the email that you have provided on the portal is up to date and actively monitored. This is to ensure that you are receiving notifications around your PCI DSS. It also ensures that if you have any problems accessing your account that it is the correct email.

Username reset

Normally your initial username is your Merchant Identification Number, if you change or reset this please ensure that you keep this somewhere accessible for future access to the portal.

Password reset

If you forget your password you can reset this by requesting a new one via the log in page. You will need access to the email account registered on the portal.

Once you have received your password, you will need to log on and enter the new password you have been sent via email. The portal will then ask you for your old password. This is the one we have just emailed to you.

It will also ask you for a new password and to retype that password in the 'confirm password' field.

You will need to ensure your new password has at least one capital letter, one numeric and a symbol.

We will never ask you for your password, so please keep this confidential.

Rules for storing card data

What are the rules?

Card data can only be stored if it is encrypted in accordance with the parameters of PCI DSS.

What are the rules around storing CAV2/CVC2/CVV2/CID?

The storage of any of this type of cardholder data (commonly called Card Security Code) is strictly prohibited by all card schemes.

This is the three digit number on the back of most of the card brands in the signature space and in the case of American Express it is on the front of the card.

What if I need to store other customer card data for recharges?

In the case that your business charges for a subscription or other recharges and you have your customer's permission to retain their payment card details. You may only do so in a secure manner. This means ensuring the following:

- If you need to keep your customers' card holder data, you must make sure it is protected in accordance with the PCI DSS.
- This means that you need to ensure that you securely store and encrypt data on the computers you use in your business for more details see Requirement 3 of the PCI DSS.
- You are not allowed to store sensitive authentication data (full track data, card validation code or value, and PIN data) this is strictly forbidden by the PCI DSS.

What are the rules for businesses taking payments through call centres and storing information?

It is strictly prohibited for any business to store any sensitive authentication data, including Card Security Codes and values after authorisation, even if they are encrypted.

If your call centre uses any form of digital audio recording you may not under any circumstance record and store CAV2, CVC2, CVV2 or CID codes in formats such as wav, mp3 etc.

Where technology exists to prevent recording of this information, this technology will need to be enabled.

How do compensating controls apply to PCI DSS?

A compensating control can be allowed as a substitute for a PCI DSS requirement if a business is able to prove that they are unable to meet a certain requirement. This can be due to technical restrictions or a specific, and documented business constraint. These controls must reduce the risk, the business or organisation must prove that they have reduced the risk of not meeting a certain requirement and also have this compensating control reviewed, approved and signed by an approved QSA.

What if I cannot meet a specific requirement due to legitimate business reasons?

If certain requirements cannot be met, the risk must be reduced or mitigated by implementing what is referred to as compensating controls. A compensating control must be approved and signed by an approved QSA

There are a number of different criteria that need to be satisfied if compensating controls are needed.

1. They must meet the intent and rigor of the original PCI DSS requirement.
2. The compensating control must provide the same level of defence to the business as the original PCI DSS requirement. For more information on what the intention around each PCI requirement is and to understand this in more detail visit www.pcisecuritystandards.org
3. Go above and beyond other PCI DSS requirements. This means that simply being in compliance is not enough and is not considered a compensating control. How do you go above and beyond? Consider the following:
    - All compensating controls must be reviewed and validated by an assessor conducting a PCI DSS review.
    - The effectiveness of a compensating control depends on the specifics of the environment, surrounding security controls and how systems are configured.

Be aware that particular compensating controls are depended on the business environment, it is not a one size fits all.

How does this work? A few examples below to help clarify this.

Existing PCI DSS requirements are not and CANNOT be considered as compensating controls if they are already required for an item under review.

An example of this may apply to the sending of passwords for non-console administrative access, these must be encrypted to reduce the risk should they be intercepted. Using other PCI DSS password requirements such as user lockout, complex passwords etc. does not reduce the risk of sending unencrypted clear text passwords.

The solution? In certain cases, existing PCI DSS requirements may be considered as compensating controls if they are required for another area but are not required for the item under review.

An example of this, relating back to the previous example – two-factor authentication is required for remote access but not for internal network transmission. The use of a two-factor authentication may be considered as a compensating control for non-console administrative access when encrypted transmission of passwords cannot be supported. In this case the compensating control meets the intent of the original requirement by:

1. Addressing the risk of intercepting clear text administrative passwords
2. It is properly set up in a secure environment.

The compensating controls must be proportionate with the additional risk by not adhering to the PCI DSS requirement. The assessor is required to thoroughly evaluate any compensating control during each annual PCI DSS assessment. To maintain compliance – processes and controls must be in place to ensure that the compensating controls remain effective after the assessment is complete.

What are PIN Transaction Security Requirements?

These are a set of security requirements that manufacturers of devices use for processing cardholder PINs and other payment processing related activities. The requirements provide manufacturers with guidelines on how the devices should be designed, manufactured and transported.

Any organisation processing card details should only use devices or components that are tested and approved by the PCI SCC.

Ecommerce Site

Understand how your site is set up

For online retailers and businesses with an ecommerce website it is important to understand how your website is set up. You need to know who your hosting provider is. How your website is set up to accept payments and if you have a shopping cart function, among other things. There are numerous ways in which your ecommerce site can be set up and each one has a slightly different risk level.

Some of the factors are listed below, you need to consider how your ecommerce site is set up, if it is one of the following:

- Content management system with shopping cart plug in
- Integrated ecommerce content management system
- Click and go website builder with a fully hosted ecommerce solution
- Click and go website builder with shopping cart plug in

You will need to provide us with the following information:

- Who your web hosting provider is
- The name of your shopping cart plug in if you have one
- If you have an ecommerce content management system you will need to provide us with the name of this and if it is hosted or if you use a different hosting company.

If you use a third party to accept payment card information, you will need to provide us with their name.

Payment service providers

A payment service provider offers online services for accepting electronic payments by a variety of payment methods.

A payment service provider will connect directly inwards into your merchant bank account. They normally provide and fully manage the technical connection between your customer and your merchant bank account.

This is often referred to as a payment gateway which allows customers to pay for a product or service online via an ecommerce site, with the money deposited directly into your merchant bank account.

Payment service providers may also allow for alternative payments such as bank transfer or digital wallets, however only ones that relate to collecting of payment cards are relevant for your PCI DSS requirements.

Payment applications

A payment application is any third party software that stores, processes or transmits card data electronically. Any payment application software that you use must be PA-DSS validated.

All PA-DSS validated software is listed on the PCI DSS website
https://www.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement

Barclaycard keep pushing me to become PCI DSS compliant, but are Barclaycard compliant themselves?

As a card acquirer, Barclaycard have always been held to the highest possible standards by Card Schemes (e.g. VISA, MasterCard) and are subject to the highest level of compliance checking and evidencing/auditing.

In the same way that merchants are required to re-assess and confirm their compliance, we are running a continuous detailed end-to-end audit assessment to evidence that our status continues to meet the card acquirers' requirements for the PCI DSS standard as specified by the Card Schemes.

This also includes confirmation that the status of all our relevant third parties complies with the PCI DSS requirements for card acquirers.

At Barclaycard we take data security extremely seriously. As the leading light in payment technology we understand the need to adhere to the strictest levels of legal checking and auditing around storing and transferring cardholder data.

As part of the industry level Payment Card Industry Data Security Standard (PCI DSS), we at Barclaycard have been working closely with the PCI Security Standards Council and the Card Schemes (VISA and MasterCard) to provide customers with a secure and stable payment network.

Barclaycard will remain best in class in the provision of online payment services, and our online payments system e-PDQ was ratified PCI DSS compliant since 2007. We re-validate our compliance every year.

In addition, and in accordance with our general obligations regarding data security beyond card scheme requirements, we confirm that Barclaycard will be responsible for the security of card data under its control. Barclaycard acknowledges responsibility for the security of all cardholder data it holds and processes and will be fully liable for any breach of security which is attributable to its own acts or omissions.