

Payment Processing European Acquiring:

PCI DSS Compliance
Frequently-Asked Questions

Version 2.1
Last Update 19-01-18

Important Information

- The contents of this guide form part of your contract with Paysafe. Failure to comply may result in the termination of our contract (the “Merchant Terms”).
- This guide covers core acquiring services requested by your business on your original application form, as well as other options you may not have selected. For more information about other products and services, such as alternative payment methods, please contact uk.customerservice@paysafe.com
- You must only accept card payments for goods and services as detailed in your original application form, or with prior written agreement from Paysafe.

Contents

- 1. WHAT IS PCI DSS 4**
 - 1.1 WHO NEEDS TO BE COMPLIANT WITH PCI DSS 4
 - 1.2 WILL PAYSAFE HELP ME BECOME COMPLIANT 4
- 2. WHY DO I NEED TO BECOME PCI COMPLIANT? 4**
 - 2.1 WHAT HAPPENS IF I AM NOT COMPLIANT 4
 - 2.2 WHAT IF I AM USING A 3RD PARTY SOFTWARE 5
 - 2.3 HOW OFTEN DO I HAVE TO COMPLY WITH PCI 5
 - 2.4 I HAVE COMPLETED AND VALIDATED MY COMPLIANCE WITH ANOTHER COMPANY – DO I NEED TO DO IT AGAIN? 5
 - 2.5 HOW MUCH DOES IT COST TO BE PCI COMPLIANT? 5
- 3. WHAT DO I HAVE TO DO 6**
 - 3.1 WHY DO YOU NEED MY PROFILE? 6
 - 3.2 WHAT IS A SELF-ASSESSMENT QUESTIONNAIRE (SAQ)? 6
 - 3.3 WHAT IS ASV SCANNING? 6
- 4. OTHER FREQUENTLY-ASKED QUESTIONS 7**
 - 4.1 WHO SENDS ME DETAILS ABOUT BECOMING COMPLIANT? 7
 - 4.2 HOW LONG WILL IT TAKE TO RECEIVE MY LOGIN CREDENTIALS? 7
 - 4.3 I STILL HAVE NOT RECEIVED MY LOGIN CREDENTIALS, WHAT DO I DO? 7
 - 4.4 WHAT ARE THE HOURS OF OPERATION FOR THE PAYSAFE PCI TEAM? 7
 - 4.5 HOW DO I ACCESS THE PAYSAFE PCI PORTAL? 7
 - 4.6 MY PASSWORD DOES NOT WORK, WHAT DO I DO? 7
 - 4.7 WHAT DO I DO IF I AM ALREADY COMPLIANT? 8
 - 4.8 4.8 WHAT HAPPENS IF I DON'T BECOME PCI COMPLIANT? 8
 - 4.9 WHICH SAQ SHOULD I TAKE? 8
 - 4.10 CAN PAYSAFE COMPLETE THE SELF-ASSESSMENT QUESTIONNAIRE FOR ME? 8
 - 4.11 I COMPLETED PCI WITH ANOTHER SERVICE PROVIDER FOR PCI COMPLIANCE. CAN I JUST SEND YOU MY CERTIFICATION?
8
 - 4.12 WILL I RECEIVE A PCI RENEWAL REMINDER? 8

1. What is PCI DSS

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 organizations processing credit and debit card payments to ensure controls are in place to prevent fraud.

The PCI DSS standard applies to all organizations accepting, processing and or storing cardholder information from the card brands.

1.1 Who needs to be compliant with PCI DSS

Any organization, regardless of size or quantity of transactions, that accepts, stores, process or transmits payment card data by card brands must be PCI Compliant.

1.2 Will Paysafe Help Me Become Compliant

Paysafe have set up the PaysafePCI portal in partnership with Sysnet, a company that specializes in Data Security and Compliance. Logging on to the PaysafePCI portal will allow you to complete the assesment. Sysnet are on hand to provide the support for Paysafe merchants who need to achieve PCI compliance.

2. Why do I need to become PCI Compliant?

If you take card payments from your customer's you must do so safely to protect your customers' payment card information. The PCI DSS standard was developed by the card brands to make sure that businesses understand what safely means and follow the guidelines required to prevent fraud.

2.1 What happens if I am not compliant

If you are not compliant and there is a data breach where card data is stolen you will be expected to cover the full cost, all on your own. The significant cost of paying for a breach could be potentially devastating for your business. The portal was designed to make the user experience as easy and straight-forward as possible.

Breach related costs normally include chargebacks, 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. Customers will lose trust in your business and the loss of business caused by a damage to your reputation, this can be difficult to put a figure on.

2.2 What if I am using a 3rd Party Software

Even if you use or outsource cardholder data functions to a third-party service provider you are not excluded from PCI compliance regulations. You must still complete an assessment as there are still behaviors and risk factors under your control that must be assessed.

2.3 How often do I have to comply with PCI

You are required to validate and report your compliance once a year. With that said, you are expected to be compliant all year round.

In addition, depending on the specific way in which you accept payments, you may also be required to do a system scan every three months.

2.4 I have completed and validated my compliance with another company - Do I need to do it again?

You are still required to enrol and upload your documents in this program, however you will not be asked to complete the security assessment section. You will be required to provide a copy of your self-assessment validation certificate, your Attestation of Compliance and any scan results which will have been issued to you by your QSA.

2.5 How much does it cost to be PCI compliant?

Currently there are no fees to enrol to the Paysafe PCI program. Paysafe wants to provide our customers with the best opportunity to become compliant and ensure that your customer's data is protected and secure. All customers have 90 days to become compliant, however failure to comply will attract a non-compliance fee of £40 per month (or currency equivalent) for each MID a merchant operates that is not PCI DSS compliant.

If a merchant transitions from being compliant to being non-compliant; this fee will not be charged for the first 90 days of non-compliance.

3. What do I have to do

The portal was designed to make the user experience as easy and straight-forward as possible. There are just three steps to complete on the portal to validate your PCI Compliance:

The portal was designed to make the user experience as easy and straight-forward as possible.

- Answer basic questions to establish your company profile
 - This helps us to understand which risk factors and questions are relevant.
- Complete your security assessment which will involve a series of questions and in some cases scanning of the computer systems within your business.
- Confirm and validate the information provided is correct, officially referred to as Attestation of Compliance.

3.1 Why do you need my 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.

3.2 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 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.

Sysnet is the approved QSA for managing the completion of the PaysafePCI program SAQs. Sysnet maintain a clear and concise user portal that allows merchant to be accurately profiled and complete the correct SAQ. Sysnet will automatically send reminding emails to advise when the annual revalidation date is approaching.

3.3 What is ASV scanning?

ASV stands for Approved Scanning Vendor and the scan is a system check that verifies any vulnerabilities.

Sysnet is the ASV provider for the PaysafePCI program. Consistent with Sysnet's management of the SAQ process, they will send reminding emails when scanning dates are approaching and will provide merchants with details of the ASV scan results; a clean ASV scan must be achieved and validated to every three months to achieve and maintain your compliance.

Not all merchants are required to complete an ASV scan. You will need to complete the scan if you fit into one of the following criteria:

- Your payment terminal is connected via an internet cable
- You host a payment page and/or transmit payment card data via an API link
- You store credit and/or debit card numbers electronically (even if only momentarily)

4. Other Frequently-Asked Questions

This section covers various other bits of information you may wish to know.

4.1 Who sends me details about becoming compliant?

When Paysafe sets your merchant, account live we also register your details with our partner Sysnet. Sysnet will get in touch with you via no-reply@pcidssportal.com to provide you with your user credentials and instructions on where to log into.

4.2 How long will it take to receive my login credentials?

Usually this is received within three workings days.

4.3 I still have not received my login credentials, what do I do?

If the three-business day timeframe has passed and you have not received your credentials, please contact the Paysafe PCI team by phone at 0800 294 1404 or +44 (0) 118 928 5075.

4.4 What are the hours of operation for the Paysafe PCI team?

They are available Monday through Friday, 8:00 AM through 8:00 PM.

4.5 How do I access the Paysafe PCI Portal?

You can follow the instructions provided in your email, or sign up by visiting <https://paysafe.pcidssportal.com/safemaker/login/>

4.6 My password does not work, what do I do?

Please contact the Paysafe PCI team by phone at 0800 294 1404 or +44 (0) 118 928 5075.

4.7 What do I do if I am already compliant?

Please log on and provide a copy of your self-assessment validation certificate, your Attestation of Compliance and any scan results which will have been issued to you previously. This will ensure our records are complete and fines avoided.

4.8 4.8 What happens if I don't become PCI compliant?

Failure to comply with the mandate will result in a fee that will be assessed monthly until you become PCI Compliant. This fee is in effect starting (90) days after becoming non-compliant or from approval to commence credit and debit card processing.

4.9 Which SAQ should I take?

The best SAQ for your business will be determined during the profiling stage with Sysnet.

4.10 Can Paysafe complete the Self-Assessment Questionnaire for me?

Unfortunately, the Self-Assessment Questionnaire must be completed by the merchant or anyone employed at the merchant location to maintain the integrity of the assessment

4.11 I completed PCI with another service provider for PCI Compliance. Can I just send you my certification?

Please send any PCI document(s) to Paysafepci@paysafe.com and provide your Merchant ID and Merchant Name as reference. Our Compliance team will review the document(s) and perform the offline upload to the portal if the documents are valid.

4.12 Will I receive a PCI renewal reminder?

PCI SAQ's expire annually and whilst you will receive advanced warning for certification expiry, it is your responsibility to ensure you also keep a record of renewal.

Depending on which SAQ is taken, a quarterly scan may also be required and is included with the SAQ. These quarterly scans must be renewed every 90 days, again you will receive notification to action.