Reset

Payment Services

Checklist for reviewing PCI DSS compliance

The merchant is required to secure all systems and data carriers that contain card data (see section 13 of the GBCs) from loss or access by unauthorized third parties. The merchant is also obligated to meet all the requirements of the international card organizations and SIX Payment Services, particularly the PCI DSS guidelines, at all times.

The details below relating to the company must be provided if at least one of the three PCI questions in the contract has been answered with "no" or "not applicable".

Company details

Company

Street/No. | Country

Postal code/City | Merchant number

Please provide us with information about the hardware and software types you work with, as well as who within your company was responsible for setting up the cash register solution.

Cash register integrated solutions

Manufacturer/Brand

Type | Serial number

Software (version number)

☐ PCI-certified ☐ not PCI-certified

Cash register integrator

Company

Street/No.

Postal code/City

Country | Phone

Terminal/POS device

Manufacturer/Brand

Type | Serial number

Terminal ID

Software (version number)

☐ PCI-certified ☐ not PCI-certified

Other solutions

Manufacturer/Brand

Type | Serial number

Software (version number)

☐ PCI-certified ☐ not PCI-certified

Other integrations

Manufacturer/Brand

Type | Serial number

Software (version number)

☐ PCI-certified ☐ not PCI-certified

Confirmation readiness attaining PCI DSS compliance

Hacking attacks against IT systems and settlement systems for card payments have increased dramatically in recent years, including incidents in which millions of cardholder data have been stolen. This has led to considerable losses and damage incurred by all involved parties. With the introduction of the Payment Card Industry Data Security Standard (PCI DSS), the leading card organizations (Visa, Mastercard, American Express, JCB and Discover) seek to further enhance the security of card payments and thereby even more effectively protect merchants and cardholders from the theft and misuse of card data.

All merchants worldwide that transmit, process or store card data are obligated to adhere to the Payment Card Industry Data Security Standard (PCI DSS) defined security guidelines. If these guidelines are not followed, then the card organizations can levy penalties and claims for loss compensation. As a direct consequence of such a case, SIX Payment Services may be compelled to terminate an existing contract relationship without notice and to claim payment of the penalties and loss compensation claims from the merchant involved.

In addition to complying with the security guidelines for their own systems and applications, merchants are also responsible for ensuring that their assigned third-party companies, such Payment Service Providers (PSP) or Data Storage Entities (DSE), which transmit, process or store card data on their behalf, adhere to the security guidelines.

Fundamentally, it is in the interest of each merchant to implement and adhere to the PCI DSS security guidelines. The card organizations require the contract providers (acquirers) – in your case this is SIX Payment Services – to ensure that each of their merchants adhere to the PCI DSS guidelines. This also includes having merchants declare the security measures they have taken (certification). The scope of this declaration (certification) depends on the number of transactions processed and whether the merchant comes into contact with card data during the transmission, process or storing thereof.

The merchant hereby confirms that they will complete the Self-Assessment Questionnaire (SAQ) on the SAQ Web portal * and conduct the certification if they are requested to do so in writing by SIX Payment Services. Furthermore, the merchant agrees to adhere to the stipulated deadlines.

Place/Date

Company

The signatory's first and last name(s) (in block letters)

The merchant's legal signature

* The SAQ Web portal is intended to enable SIX Payment Services merchant's to conveniently complete the declaration of their security measures online according to the PCI DSS security guidelines.

Your local point of contact can be found at: www.six-payment-services.com/contact

SIX Payment Services Ltd
Hardturmstrasse 201
P. O. Box
CH-8021 Zurich

SIX Payment Services (Europe) S.A.
10, rue Gabriel Lippmann
5365 Munsbach
Luxembourg

SIX Payment Services (Austria) GmbH
Marxergasse 1B
1030 Vienna
Austria

SIX Payment Services (Germany) GmbH
Langenhorner Chaussee 92-94
22415 Hamburg
Germany

110.0114.02 INT_EN/03.2018