PCI DSS compliance instructions Security standards for merchants

All merchants worldwide that transmit, process or store card data are required to comply with the security guidelines defined in the Payment Card Industry Data Security Standard (PCI DSS). If these guidelines are not observed, PostFinance is entitled to terminate the contractual relationship with immediate effect and to claim compensation for any claims or penalties incurred.

As technical and organizational guidelines, the following directives are binding components of the acceptance agreement with regards to Combo payment methods with PostFinance.

What does PCI DSS cover?
PCI DSS encompasses twelve mandatory requirements aimed at protecting card data during processing, storage and transmission. PCI DSS is implemented through the security programs of the card organizations. These include AIS from Visa, SDP from Mastercard® and the equivalent programs from AmericanExpress, Discover (Diners Club) and JCB.

Why was PCI DSS introduced?
The theft of card data has steadily increased in recent years. The fraudulent use of stolen card data has caused significant losses for all parties involved.

What is the purpose of PCI DSS?
With PCI DSS, the card organizations seek to further enhance the security of card payments to protect merchants and cardholders, as well as the industry as a whole, more effectively against the theft and misuse of card data.

Who is required to comply with PCI DSS?
PCI DSS requires all merchants worldwide that transmit, process or store card data to take and maintain effective security measures.

Furthermore, the merchants are responsible for ensuring that third parties they engage to transmit, process or store data on their behalf, such as payment service providers (PSPs) or data storage entities (DSE), also comply with PCI DSS.

Who is responsible for compliance with PCI DSS?
It is fundamentally each merchant's responsibility to comply with the PCI DSS security guidelines. However, the card organizations also require merchants to declare (have themselves certified) the security measures they have implemented. The scope of declaration (certification) depends on the number of transactions conducted and whether the merchant is involved in the transmission, processing or storage of card data.

What types of certification methods are there?
PCI DSS distinguishes between the following three certification methods (see also table on the next page):

- **Self-Assessment Questionnaire (SAQ)**
  This involves completing a self-assessment questionnaire.
- **Network Scan**
  An accredited certification firm (approved scanning vendor) carries out a friendly hacker attack on a quarterly basis, in coordination with the merchant, to identify possible vulnerabilities.
- **On-Site Audit**
  Merchants with large transaction volumes or those that have been the victim of card data theft are obliged to complete a report on compliance (ROC). The results must be inspected and confirmed by a qualified security assessor (QSA) or internal security assessor (ISA).

If the merchant fails to fully meet all the certification criteria, then they are required to improve the security arrangements in the relevant areas immediately.

Who bears the expenses for certification?
The costs for the certification measures are to be covered in full by the merchant or mandated third party, as are the costs for rectifying deficiencies identified during the certification process.

What happens if a merchant does not obtain certification?
If a merchant who is required to obtain certification fails to do so, then PostFinance is entitled to terminate the contractual relationship with immediate effect and to claim penalties charged by the card organizations and compensation for losses claimed by the card issuer.

Who can view the certification data?
Only the merchant and the certification company can view the data collected in the scope of the certification process. However, the merchant is obliged to send the summary of the certification results to PostFinance. PostFinance and the acquirer Worldline can also view the self-assessment questionnaires. The card organizations, on the other hand, only receive statistical evaluations.

How often must certification be renewed?
In accordance with the table on the next page, the certification measures must be periodically repeated.

Changes on the merchant side, such as the installation of new hardware or software, a new website or a change of service provider, which are associated with the acceptance of card payments, must also be reported to PostFinance immediately. In some circumstances, this may require a new certification.

Through which companies must the certification measures be conducted?
You will find a list of all accredited certification firms on the Internet:

- for the conducting of on-site audits:
  pcisecuritystandards.org/pdfs/pci_qsa_list.pdf
- for the conducting of network scans:
  listings.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.0.pdf

Where can i learn more about PCI DSS?
You can find further information about PCI DSS at the following websites:

- Worldline:
  worldline.com/merchant-services/pci
- PCI Security Standards Council:
  pcisecuritystandards.org

Who needs to take which certification measures?

Level	Description	Visa, Mastercard®/ Maestro, Diners/Discover	JCB	American Express
1	Merchants with more than 6 million transactions per year	Annual On-Site Audit [1] Quarterly Network Scan		
	Merchants after esuffering previous hacker attack with card data fraud			
	Merchants with more than 2.5 million transactions per year			Annual On-Site Audit Quarterly Network Scan
	Merchants with more than 1 million transactions per year		Annual On-Site Audit Quarterly Network Scan	
2	Merchants with 1 – 6 million transactions per year	Annual Self-Assessment Questionnaire [2] Quarterly Network Scan		
	Merchants with 50,000 – 2.5 million transactions per year			Quarterly Network Scan
3	E-commerce merchants with 20,000 – 1 million transactions per year	Annual Self-Assessment Questionnaire Quarterly Network Scan		
	Merchants with fewer than 50,000 transactions per year			Quarterly Network Scan
4	E-commerce merchants with fewer than 20,000 transactions per year	Annual Self-Assessment Questionnaire Quarterly Network Scan	Annual Self-Assessment Questionnaire Quarterly Network Scan	
	Merchants (excluding e-commerce) with fewer than 1 million transactions per year			

[1] The merchant can decide whether it would like the on-site audit to be performed with the assistance of a qualified security assessor (QSA) or internal security assessor (ISA).
[2] The SAQ must be certified by an approved internal security assessor (ISA).

On-site audits and/or network scans are mandatory only for merchants that process, transmit or store cardholder data electronically. Regardless of this, however, we do recommend that these validation measures be carried out nevertheless, especially for merchants with complex system infrastructures. While the PCI DSS guidelines are always to be adhered to by merchants, proof of such compliance must only be provided upon written request thereof by PostFinance.

PostFinance Ltd
Mingerstrasse 20
3030 Bern
Switzerland

www.postfinance.ch

460.349 en (dok.pf/pf.ch) 02.2025