
# TTS eGuide to PCI Compliance

## An Introduction

October, 2023

# Introduction

PCI compliance, or Payment Card Industry Compliance, refers to a set of 12 security standards that businesses must use when accepting, transmitting, processing and storing credit card data.[1]

As explained in the TTS eGuide to Online Payment Services one of the advantages of using a Payment Service Provider ("PSP") is that they are responsible for being PCI Compliant, not you. However, the disadvantages of using a PSP are:

- **Less account stability:** increased chance of having your account frozen or cancelled if your business is suddenly deemed too risky.
- **Volume limits:** PSPs tend to have set limits on transaction size and processing volume.

The alternative is to use a Merchant Account Provider ("MAP")[2]. However, in this case you will not only have to provide additional due diligence documentation and information to open your account, you will also have to be PCI Compliant.

# What is PCI Compliance?

PCI compliance refers to implementing and maintaining the data security requirements set out by the Payment Card Industry Data Security Standard (PCI DSS). This set of rules[3] is specifically designed to protect sensitive cardholder data when processing card transactions.

These rules were compiled by the Payment Card Industry Security Standards Council ("PCISSC"), an independent body created by the card networks in 2006. The PCISSC manages PCI security standards while the enforcement of these standards falls to the card networks and payment processors.

PCI DSS requirements apply to any entity that processes, transmits, or stores sensitive cardholder data and/or account information. Therefore, all online merchants that directly accept credit card payments must be PCI compliant.

## Four levels of PCI Compliance

PCI Compliance has four levels that are defined by the number of payment card transactions that it processes.

1. Compliance Level1: Companies processing over 6 million payments p.a.
2. Compliance Level 2: Companies processing between 1 and 6 million payments p.a.
3. Compliance Level 3: Companies processing between 20,000 and 1 million payments p.a.
4. Compliance Level 4: Companies processing less than 20,000 transactions p.a.

The higher the Compliance Level, the more stringent the checks and controls.

# What does PCI Compliance entail?

As mentioned in the Introduction, there are 12 security standards that you must implement and follow:

[1] Please note that this eGuide provides an Introduction to PCI Compliance. For more details you should visit the PCISSC site and\or check out the PCI DSS Guide.

[2] For a more complete comparison of PSP vs MAP services see the TTS eGuide to Online Payment Services.

[3] For copies of relevant documents from PCI Standards Security Council (PCI SSC) click here

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored cardholder data by masking cardholder data in databases and systems.
4. Encrypt transmission of cardholder data across open, public networks.
5. Use and regularly update anti-virus software or programs.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security for employees and contractors.

It should also be understood that:

- PCI compliance is not a one-time exercise; itis a task that must be completed each year.
- Compliance requirements vary by business size and by the number of card transactions each year.
- Compliance rules divide businesses into four groups that vary slightly by card network. For example, Visa classifies Level 4 merchants as those that process fewer than 20,000 online card transactions or up to 1 million total transactions per year. Larger businesses generally have more burdensome requirements.

## Is PCI Compliance required by law?

No. Moreover, while the PCI Security Standards Council manages security standards and looks for ways to improve security, it does not enforce compliance either. Instead, the steps a business must take to be PCI compliant are in the terms of the contract or agreement with its merchant service provider or payment service provider and the card networks.

Furthermore, while the broad intent of these requirements is the same from one provider to the next, details about implementation can vary. Not following the proper procedures as set out in the relevant service agreement contract can lead to serious problems, including tens of thousands of dollars in fines.

## How to become officially PCI Compliant

The PCI SSC provides self-assessment questionnaires. The right questionnaire for a given merchant depends on factors such as how the merchant processes transactions or which network they are using. For example, the SAQ A is for merchants that outsource all of their payment processing and transaction information, while the SAQ A-EP is for merchants that partially outsource their e-commerce payment channel to third parties validated by PCI DSS.

- **A Report of Compliance ("ROC"):** - is submitted to the acquiring bank to document the merchant's adherence to PCI DSS standards. A ROC may be completed internally by the merchant or externally by a third-party qualified security assessor (QSA), depending on the merchant's level of PCI compliance.
- **An Attestation of Compliance ("AOC"):** - is a report submitted by a third-party QSA verifying that the merchant meets the applicable compliance requirements.
- **Quarterly Network Scans:** - should be performed across the merchant's network by approved scanning vendors (or ASVs). A network scan is intended to identify any weaknesses within the merchant's network.

- **Annual Penetration Testing:** - puts a merchant's network through rigorous stress tests. Security professionals attempt to hack the merchant and gain access to sensitive information.

## PCI Compliance Service Providers

All of the above requires a large investment of time, money and infrastructure investment. It is possible to spend months analysing your data processes, storage procedures, updating infrastructure and training employees – and possibly organising an independent audit.

PCI compliance can be frustrating for business owners because it means taking on a subject — cybersecurity — they might have little expertise or interest in.

Should you still want to become PCI Compliant, it may make sense to commission a PCI Compliance Service Provider.

According to the PCI DSS Glossary of Terms, Abbreviations, and Acronyms, a service provider is a: "Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities."

See Appendix One – Third Party Service PCI Compliance.

## Conclusions

Given the resources required, PCI Compliance only makes sense if the volume of business can justify the investment.

Should the decision be made to become PCI Compliance, you will need to:

1. Complete an analysis of your current procedures and infrastructure.
2. Define the changes you will need to make – and whether to do everything internally or to use a PCI Compliance Service Provider
3. Implement those changes.

This procedure can be completed using internal or external PCI Compliance experts.

# Appendix One – Third Party Service PCI Compliance Service Providers

As a first step you may decide to can find a suitable compliance consultant on Upwork

**Cybersecurity companies specialising in PCI Compliance – with links to their web sites**

| UK Service Providers | International Service Providers |
|---|---|
| Adarma | Brezha Security Group |
| Capita | Fidelis Cybersecurity |
| Clearswift | Fluid Attacks |
| Creative Networks | H2Cber |
| Darktrace | LogicalTrust |
| Intercede | Nuformat |
| IT Governance | SecurityMetrics |
| LRQA | Skyflow |
| Microminder Cyber Security | Spreedly |
| Sapphire Cybersecurity | TestPros |
| Sophos | Triaxiom |

***N.B.*** Disclaimer. Apart from Darktrace, TTS has no commercial agreement with any of the companies.