A guide to PCI Compliance

What it is PCI compliance and why does it matter?

If you own an online shop, bank online or use credit and debit cards, there is a very good chance that you have heard the term "PCI compliant." However you probably don't know what it means.

The term "PCI compliant" is heard more and more these days as data breaches at merchants like TJMaxx land hundreds of thousands of card details in the hands of criminals. These criminals are using the data to make purchases and withdraw money from accounts of unsuspecting victims.

It's a huge and growing problem. More than 80% of data stolen in breaches is payment card data, according to the 2009 Verizon Business Data Breach Report.

Who are PCI Security Standards Council

The PCI Security Standards Council is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards, including: the Data Security Standard (DSS), Payment Application Data Security Standard (PA-DSS), and Pin-Entry Device (PED) Requirements.

What is the standard exactly?

It's the PCI, which stands for Payment Card Industry, data security standard. It's a set of 12 specific requirements that cover six different goals. It's very prescriptive. It says not only that you need to be secure but it tells you how to become secure. It's more about security than compliance. The goals are things like:

- Build and maintain a secure network
- Protect card holder data
- Regularly monitor and test the networks

What if I don't want to become PCI compliant?

If you decide not to become compliant then you can still open an account with us. However...

If you are not compliant to the Payment Card Industry Data Security Standards (PCI DSS) you will be responsible for any losses through fraud, and may also face considerable fines. Your customers will suffer if their card details are compromised. Your business reputation will suffer as a result.

Taking responsibility for PCI compliance forms part of your merchant Terms & Conditions.

If a merchant is found to be not PCI compliant, what are the consequences?

90% of consumers don't understand the difference between credit card fraud and identity theft. If they hear that their credit card has been stolen, many of them believe their identity is at risk. If that's the case many of your customers won't shop with you anymore because they are afraid you are not protecting their data and someone is going to steal their identity. That's the worst thing that can happen. The biggest problem would be if your customers walk away. There are reputational damages they have to deal with, which 9 times out of 10 cannot be measured in terms of money.

What part of the standard is mandatory and what is voluntary?

It's all mandatory. Nothing is voluntary. The rule is if you store, process, or transmit credit card data you must be compliant with the PCI standards. And that's a global rule.

How do I become compliant?

You can become compliant by using an assessor. To see the current list of PA-QSAs recognized by the PCI Security Standards Council, please see below. Alternatively search online for 'PCI compliant assessors'.

- www.trustwave.com
- www.mcafee.com
- www.srm-solutions.com
- www.ambersail.com
- www.nccgroup.com

Please note, the PCI Security Standards Council maintains an in-depth program for security companies seeking to be certified as Payment Application Qualified Security Assessors (PA-QSAs), as well as to be re-certified as PA-QSAs each year.

We do not take any responsibility for 3rd party websites and / or services

---

How much does it cost to become compliant?

If you would like help with becoming compliant, prices vary from company to company. However the average price is around £150. If you would simply like to self-assess then this is free.

Isn't this just another way of getting more money out of businesses?

Not at all. This is for the benefit of all concerned. 80% of all online fraud occurs using stolen or missused payment details. No matter where you go to become PCI compliant (except for self assessment) you will have to pay a fee.

What now?

For more information, including an FAQ's section please visit www.pcisecuritystandards.org

---

Don't let it happen to you!

€5,250 is the minimum cost of non-compliance

If you are not PCI DSS compliant, €5,250 is the least amount that the Card Schemes could fine. If fraudsters get their hands on your customer payment card data, this amount will increase.

If your data is compromised, card issuers may also require you to certify your compliance within 90 days by using a Qualified Security Assessor. Typical cost is £850 per day, with assessments taking up to two weeks

Card issuers may also insist on an investigation by a Qualified Forensic Investigator. Typical cost is £850 per day. An investigation could last for 10 days. You could also be liable for other costs, including card replacements.

Don’t be left counting the cost of non-compliance.

What could your business do with €5,250?

- Buy equipment for expansion?
- Replace aging computer equipment?
- Run a promotional advertising campaign to drive growth?
- Lease a new van?
- Spruce up your premises?
- Give bonus payments to hard-working staff – or to yourself?

Or pay a fine for non-compliance?

www.web-merchant.co.uk

Web-Merchant Services Limited
+44 (0) 845 475 3540
info@web-merchant.co.uk