The importance of...

Becoming PCI Compliant

Why should you be PCI compliant?

If your business stores, processes, or sends any payment card information then you must be PCI compliant or you could face significant fines and in some circumstances expulsion from card processing networks and cancellation of your agreement.

As a merchant your number one responsibility is to protect your customers' cardholder data and PCI compliance ensures that you implement 'best practice' across your business to achieve this.

PCI compliance may on the face of it appear time consuming and an unnecessary effort, but it is infact extremely important and may prevent future issues that could cost your business dearly.

What is PCI Compliance?

The PCI Compliance Standards are mandated by the card schemes such as Visa, MasterCard and American Express, and run by the Payment Card Industry Security Standards Council, the standard was created to increase controls around cardholder data to reduce credit card fraud.

PCI Compliance can bring your business major benefits including:

- **Customer Trust** - PCI Compliance means that you have successfully configured your systems and processes are sufficient to support the requirements set by the industry and that customers can trust you with their sensitive payment card information, if your customers trust you they are more likely to become loyal customers and recommend you to others
- **Improved reputation** - not only with your customers but with acquirers and payment card schemes

Failure to comply can have serious and consequences including:

- **Negative Publicity** - An incident can severely damage your reputation and your ability to conduct business
- **Financial Implications** - Loss of sales and customer relationships
- **Payment card issuer fines** – these could range from non compliance fines upto hundreds of thousands if you are the victim of a data breach which results in card holder loss

You have worked hard to build your business – can you afford not to be compliant and risk your business and reputation, research shows that in the UK 12% of consumers have been the subject of fraud[1]. By being PCI compliant you ensure that you are operating best practice, and support the prevention and impact of fraud originating in your business.

What do I need to do to become PCI DSS Compliant?

Your PCI requirements will depend on which merchant level you fit into, there are 4 Levels:

Level 1 - Merchants that take over 6,000,000 Visa and/or MasterCard transactions per year will be required to bring in a Qualified Security Assessor (QSA) on-site to evaluate security and create an in-depth compliance report. Quarterly PCI Scans are also required.

Level 2 - Merchants that take between 1,000,000 and 6,000,000 Visa and/or MasterCard transactions (all channels) per year must complete a Self-Assessment Questionnaire (SAQ). Quarterly PCI Scans are also required.

Level 3 - Merchants that do between 20,000 and 1,000,000 Visa and/or Mastercard e-commerce transactions per year need to complete a Self-Assessment Questionnaire (SAQ). Quarterly PCI Scans are also required.

Level 4 - Merchants processing less than 20,000 Visa and/or MasterCard e-commerce transactions annually and all other merchants processing up to 1 million Visa and/or MasterCard transactions annually need to complete a Self-Assessment Questionnaire (SAQ). Quarterly PCI Scans are also required.

PCI Compliance does not guarantee that your business will not be affected by fraud or that your website won't be hacked, but it does mean that you are operating 'best practice' as acknowledged by the card payments industry.

Types of self-assessment

There are five self-assessment the details are in the table below:

Assessment	Description	Additional Details
A	Card-not-present (e-commerce or mail/telephone-order) merchants. **This option would not apply to face to face merchants.**	▪ The merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions ▪ The merchant does not store, process, or transmit any cardholder data on their systems or premises, but relies entirely on a third party ▪ The merchant has confirmed that the third party is PCI DSS compliant ▪ The merchant retains only paper reports or receipts with cardholder data, and these documents are not received electronically ▪ The merchant does not store any cardholder data in electronic format
B	Imprint-only merchants with no electronic cardholder data storage, or standalone, dial-out terminal merchants without electronic cardholder data storage. **This option would never apply to e-commerce merchants.**	▪ The merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions ▪ The merchant does not store, process, or transmit any cardholder data on their systems or premises, but relies entirely on a third party ▪ The merchant has confirmed that the third party is PCI DSS compliant ▪ The merchant retains only paper reports or receipts with cardholder data, and these documents are not received electronically ▪ The merchant does not store any cardholder data in electronic format
C-VT	Merchants using only web-based virtual terminals, no electronic cardholder data storage **This option would never apply to e-commerce merchants.**	▪ The merchants only payment processing is done via a virtual terminal accessed by an Internet-connected web browser ▪ The merchants virtual terminal solution is provided and hosted by a PCI DSS validated third-party service provider; ▪ The merchant accesses the PCI DSS compliant virtual terminal solution via a computer that is isolated in a single location, and is not connected to other locations or systems within your environment (this can be achieved via a firewall or network segmentation to isolate the computer from other systems) ▪ The merchants computer does not have software installed that causes cardholder data to be stored ▪ The merchants computer does not have any attached hardware devices that are used to capture or store cardholder data ▪ The merchant does not otherwise receive or transmit cardholder data electronically through any channels ▪ The merchant retains only paper reports or paper copies of receipts; ▪ The merchant does not store cardholder data in electronic format.
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage If you have a face to face terminal you are more than likely going to need to complete this self-assessment	▪ The merchant has a payment application system and an Internet connection on the same device and/or same local area network (LAN) ▪ The payment application system/Internet device is not connected to any other systems within your environment ▪ The merchant is not connected to other store locations, and any LAN is for a single store only ▪ The merchant retains only paper reports or paper copies of receipts ▪ The merchant does not store cardholder data in electronic format; ▪ The merchants' payment application software vendor uses secure techniques to provide remote support to your payment application system.
D	All other merchants not included in descriptions for SAQ types A through C above, and all service providers defined by a payment brand as eligible to complete an SAQ.	

PCI DSS compliance may appear on the face of it to be an additional cost and baffling exercise but it is absolutely necessary as the penalties for non-compliance can be severe and it's important you operate 'best practice'. Think of PCI DSS compliance as additional business insurance, an essential part of doing business.

Your reputation could be damaged if your customer data is breached and can result in costly legal action, it is therefore important to ensure that you are PCI DSS compliant.

Here is our guide to keeping your customers data safe:

Regularly change your passwords – it is important to regularly change all of your passwords and ensure that you use a mixture or letters, numbers and symbols, so that it's harder for someone to guess them.

Ensure you are PCI DSS compliant – It may seem like an onerous task but PCI compliance is there to protect customers. If a data breach occurs shoppers have to cancel their cards and order replacements and at the same time the business must undergo investigation to refortify its payment system, this can take up to six months, in some cases small businesses have been forced to close because of the costs.

Train your staff to follow PCI DSS procedures – It is important that every member of your team who are taking payments understands the procedures and adhere to them.

Test your firewalls at least every six months – If you are operating an online business or are storing and customer data it is important that you have an up to date system. Testing your firewall will help you identify any breaches and whether you need to upgrade, or get a security professional to test them for you?

Destroy all card data files immediately - Always shred sensitive information. Be careful with any documents or contracts. Remove all sensitive materials from your work area when you're not using them or at the end of the day and if required lock them away.

FAQ's

1. I only accept cards over the phone does PCI still apply?

   Yes. All businesses that store, process or transmit payment cardholder data must be PCI Compliant.

2. I have a multi-site business, is each location required to validate PCI Compliance?

   If your business locations process under the same Tax ID, then typically you are only required to validate once annually for all locations

3. What should I do if I'm compromised?

   We recommend following the procedures outlined by Visa [Click here]

   If you have a QSA you should immediately contact them

4. How do I prove to the acquiring banks that I am PCI compliant?

   Once you complete your self- assessment you will be issued with a certificate. The length of validity of your PCI compliance certificate depends on whether your business requires a self-assesment questionnaire or a regular scan.

   If your business only requires the annual questionnaire then your PCI Certification is valid for one year.

   If your business requires quarterly scans, PCI Certification is valid for three months at which time your next quarterly scan will be due.

[1] http://www.theukcardsassociation.org.uk/plastic_fraud_figures/index.asp

NetPay Merchant Services

Ireland

T +353 (0)1 447 5299
E getintouch@np.ie
W www.np.ie