Payment Card Security

PCI DSS

What is the PCI DSS?

The major players in the credit card business (Visa, MasterCard, American Express, Discover and JCB) came together in 2006 to reduce credit card data loss. The payment Card Industry Security Standards Council was created and that council established a standard for the security of card holder data. The PCI Data Security Standards (PCI DSS) was born.

The Council has no legal authority, but ultimately if your business wishes to accept credit card (or debit card) transactions, then it will be required to adhere to the standards.

PCI DSS applies to any organisation that stores, processes, or transmits cardholder data and covers security for any system components included in or connected to a merchant's cardholder data environment.

Compliance with the standards can bring major benefits to businesses of all sizes, while failure to comply can have serious and long- term negative consequences.

Compliance means your systems are secure, and customers can trust you with their sensitive payment card information.

It is an ongoing process, not a one- time event. It helps prevent security breaches and theft of payment card data, not just today, but in the future.

The requirements for validating the compliance of your business vary based on the number of card transactions you process annually. All merchants are required to validate their compliance on a yearly and sometimes quarterly basis.

But if you are not compliant, it could be disastrous. Even one incident can severely damage your reputation and your ability to conduct business effectively, far into the future. A breach could have a significant impact on your business.

What if I am not PCI DSS Compliant?

Failure to meet compliance standards, resulting in a compromise of your systems, can result in fines from credit card companies and banks, it could even result in the loss of the ability to process credit cards. You could face penalties and fines ranging from $5,000 to $500,000. The fines, however, are just the beginning of the overall damage caused by noncompliance.

If you are in such a position as to lose the ability to accept and process credit card payments, you will also be placed in the Visa/MasterCard Terminated Merchant File (TMF), making you ineligible to obtain another merchant account, for at least several years. The TMF, is essentially a BLACKLIST from which it is almost impossible to be removed.

If a merchant is deemed to be compliant at the point at which a compromise occurs, the potential fines from the card brands may be waived if full compliance can be demonstrated during a forensic investigation.

Do I need to worry about PCI DSS Compliance?

Anyone who has a business that receives payments from customers who use their credit cards to pay needs to be PCI compliant – even if you only receive one credit card payment per year.

PCI does not only apply to ecommerce, it applies to every company that stores, processes or transmits cardholder information, including retail point- of- sale services and mail/phone order. In fact anyone who takes card present transactions that involve POS devices is typically more at risk than e-commerce solutions. Quite often these types of transactions involve storage of track data (which is forbidden under PCI).

Payment Card Security

PCI DSS

Be informed...

So as a company that deals with card payments, do you meet all of the necessary requirements of the PCI standards?

- Do your staff know what they must and must not do when dealing with card payment information?
- Do you know why you should be PCI compliant?
- Has your Acquiring Bank ever asked about your PCI Compliance Status?
- Are you aware of the potential consequences of not being PCI compliant?
- Do your staff follow any formal procedures when dealing with card payments from customers?
- Does your company receive emails or any paper forms containing card data?
- If Point of Sales devices are used to take card payments, are receipts stored securely; during the day, at night?
- Does everyone have access to the card payments system?

Should you be uncertain about any of the above, you need to take a moment to understand that you may be unnecessarily exposing your company to the possibility of breaching the PCI DSS?

So what do you need to do?

You need to ensure that your staff, at all levels, are made aware of the need to maintain the security of card payment data and ensure that if it is required it is kept safe and secure, and if it is not needed, it is removed and destroyed in a safe and secure manner.

About Security Risk Management Ltd

SRM are security specialists who cover the full scope of the Governance, Risk and Compliance agenda; for example information assurance to Payment Card Industry Data Security Standards (PCI DSS), HM Government Information Assurance Standards (HMG IAS), N3 (NHS private data network designed to ensure patient data security) and ISO 27001 standard for Information Security best practice, including business continuity, operational and technical risk management, training, education and computer forensics. SRM also have a number of CESG Listed Advisor Scheme (CLAS) Consultants.

This broad portfolio allows SRM to provide a more efficient and effective service, making the most of consultants' skills and offering our clients better value for money.

SRM experts, drawn from the private sector, police service, armed forces and government agencies, offer an exceptional skill-set and depth of experience, who deliver a first-class level of service.

Our existing clients, who range from small and medium size businesses to government departments, charities and other non-commercial institutions, trust SRM because we deliver what we promise.

Head Office

Security Risk Management Ltd, The Grainger Suite, Dobson House, Regent Centre, Gosforth, Newcastle upon Tyne, NE3 3PF

Tel: **08450 21 21 51**
Web: **www.srm-solutions.com**

@srm_team