RISK INSIGHTS

Crendon Insurance Brokers

Payment Card Industry Compliance

It has become commonplace for consumers to purchase goods and services with debit or credit cards rather than cash. However, this convenience may not only expose consumers to potential risks, but your business as well. To help protect both your company and your customers, as well as remain compliant, it is critical that your company understands the payment card industry data security standards (PCI DSS).

PCI DSS Overview: What You Need to Know

The PCI DSS is a set of requirements designed to ensure that all entities that process, store or transmit payment card information maintain a secure environment. The PCI DSS establishes a minimum set of requirements for protecting cardholder data. Whether you process one credit card per year or 1 million, you must follow the PCI DSS.

In addition, local laws and regulations may require specific protections for personal information or other data elements. Therefore, the PCI DSS does not supersede or replace local or regional laws, government regulations or other legal requirements.

Failure to comply with the PCI DSS, though, could jeopardise customer relationships following a data breach. Brand loyalty and trust can be easily lost—especially when you are responsible for protecting personal data from cyber criminals.

There are 12 high-level PCI DSS requirements:

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data.
2. Do not use supplier-supplied details for system passwords and other security parameters.

The United Kingdom is the largest payment card market in the European Union, according to the UK Cards Association.

Protect Cardholder Data

3. Protect stored data (use encryption).
4. Encrypt transmission of cardholder data and sensitive information across public networks.

Maintain a Vulnerability Management Programme

5. Use and regularly update anti-virus software.
6. Develop and maintain secure systems and applications.

Implement Strong Access-control Measures

7. Restrict access to data by an individual need-to-know basis.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data.

11. Regularly test security systems and processes.

Maintain an Information Security Policy

12. Maintain a policy that addresses information security.

For more specific information on PCI DSS compliance, click here. Please be aware that this guidance is not an adequate substitute for contacting a specialist and implementing your own PCI DSS programme standards. Experts recommend that you contact your acquirer, which is the entity that issued your payment processers, to clarify steps towards compliance.

The Benefits of Accepting Payment Cards

If you do not currently accept payment cards, here are five potential benefits of allowing customers to pay with cards:

- Payment cards can legitimise your business and help you build a sense of trust with customers.
- Payment cards can expand your amount of potential customers, which could then boost your revenue.
- Payment cards increase the likelihood that customers will make an impulse purchase.
- Payment cards generally encourage customers to make larger purchases.
- Payment cards are processed more quickly than money orders or checks, which may provide a boost to your cash flow.

Additional PCI Services to Consider

In addition to providing authorisations for card transactions, acquirers can also provide extra services to make it easier for you to do business, including, but not limited to, the following:

- **Address verification service and card security service:** These fraud prevention tools are installed in a payment card terminal and used to detect common types of card-not-present fraud.
- **Code 10:** If employees are suspicious of a cardholder, the payment card or the circumstances concerning the purchase, they can make a Code 10 call to your card authorisation centre. The operator will then guide them through a series of 'yes' or 'no' questions to help them determine the best way to navigate the situation.
- **Dynamic currency conversion:** This service offers holders of foreign-issued payment cards the option to be charged in their native currency at the point of sale by using up-to-date currency exchange rates, or to pay in pound sterling.
- **Multi-currency:** This service allows your company to accept non-sterling transactions, which is especially useful if your company intends to accept online transactions from international customers.
- **Recurring transactions:** Your company has the ability to set up recurring customer payments.

Payment Card Industry Compliance

Potential PCI Risks

Despite all the ways in which accepting payment cards can help grow your business, it is not risk-free. It is important that you understand the potential risks your company could encounter, which include, but are not limited to, these five common PCI risks:

1. **Untrained employees:** Staff should understand the rules for accepting cards—untrained staff can make mistakes and cost you money.
2. **Counterfeit cards:** Generally, the magnetic strip on counterfeit payment cards will appear rough and not work when swiped at the terminal. Also, the shape and format of the numbers may appear incorrect. Not spotting fake cards can be costly.
3. **Failing to match signatures:** Employees should check that the cardholder's signature matches the one on the back of the card when necessary.
4. **Storing cardholder data:** All cardholder data must be encrypted, stored and transferred securely. Neglecting to do so could ruin your business.
5. **Authorising false refunds:** Fraudsters often try to obtain cash refunds for card transactions. Ensure that all staff know how to correctly make refunds, or risk being responsible for pricey chargebacks.

Mitigating Potential PCI Risks

Fortunately, the solutions for addressing the risks associated with accepting payment cards are simple:

- Provide thorough training on properly handling payment card transactions. This could include what to do if a customer or payment card seems suspicious, and the process for accepting returns.
- Review the PCI DSS requirements annually to ensure your compliance. Use the PCI DSS annual compliance checklist, which can be found here: www.theukcardsassociation.org.uk/security/PCIDSS_checklist.asp.
- Choose a payment card system password that is at least seven characters long, with both upper and lowercase letters, symbols and numbers. Reset your password at least every three months.
- Incorporate additional PCI services, such as Code 10, to more adequately protect your business and your customers' data.

The above list is not comprehensive, but it should provide your company with a foundation on which you can incorporate additional risk prevention processes.

Charge with Confidence

As payment cards have become a necessary business standard, your company needs to be aware of the PCI DSS in order to establish a secure and efficient payment card system. To find out more about how your company can protect itself from the potential risks associated with accepting payment cards, contact **Crendon Insurance Brokers Ltd** today.