What is PCI DSS?

Natasja Bolton, Consulting Manager

November 11th, 2013

The Payment Card Industry Data Security Standard (PCI DSS) is a compliance standard that defines data security requirements relating to the processing, storage or transmission of cardholder data.

The PCI DSS was founded in December 2004 by 5 major card brands – Visa, MasterCard, American Express, Discover and JCB. In 2006, the card brands formed the PCI Security Standards Council (PCI SSC), an independent council established to maintain and update the PCI standards. The PCI DSS is now on its 4th major release.

The standard was agreed by the major card brands as a common, consistent and secure minimum level of protection to be applied by all organisations that process, store or transmit cardholder data to safeguard payment card data and payment card customers. PCI DSS applies to card payments accepted in person, over the phone or online.

PCI DSS was developed in response to the ever increasing impact and costs of payment card fraud. By 2004 annual fraud losses on UK-issued cards had reached £504.8 million but by 2011 losses had dropped to £341.0 million despite the continuing growth of card use and transaction volumes[1]. A large part of this drop can be attributed to the improved data security practices implemented by merchants as they achieved PCI DSS compliance.

Why Do Merchants Need To Worry About PCI DSS?

Any organisation which processes, stores or transmits cardholder data is required to comply with PCI DSS. Compliance is not a legal requirement; it is driven by the contractual agreements between merchants and acquiring banks.

Compliance is mandatory for any merchant that accepts payment cards. All acquirers, including First Data Merchant Solutions, are required by the card brands to enforce PCI DSS with their merchants. Even if the merchant only takes payment over the phone, uses a third party for all payment processing services and doesn't retain any cardholder data, PCI DSS applies and the merchant must assess their security against the PCI DSS requirements on an annual basis and maintain compliance with PCI DSS at all times.

PCI DSS validation and reporting requirements differ according to card brand defined merchant levels. Merchant levels are defined by the total number of annual transactions and determined by the acquirer. Merchants that process more than 6,000,000 Visa or 1,000,000 MasterCard transactions per year and/or meet the Level 1 criteria of another Card Scheme must validate their compliance with PCI DSS via an onsite Security Assessment and submit a completed Report on Compliance (ROC). This also applies to any organisation that has suffered a card data security breach over the past 12 months.

The validation tool for merchants at the lower levels is the Self-Assessment Questionnaire (SAQ), supported by external network scan results (if applicable). There are five SAQ categories (A to D plus C-VT), selection of which depends on how the merchants accept payment cards.

[1] Source: 'Fraud, The Facts 2012: The definitive overview of payment industry fraud and measures to prevent it', Financial Fraud Action UK

There are consequences if merchants do not achieve and maintain PCI DSS compliance. Acquirers are unable to allow merchants that refuse to comply with PCI DSS to continue taking card payments, as compliance is mandated by the card brands.

During the period of non-compliance the merchant may be liable for damages that may result from a cardholder data compromise. Costs in the event of a data breach may include fines levied by the acquirer, increased compliance costs (as PCI DSS validation requires a full onsite Security Assessment) and consultancy costs for forensic assessments and remediation. Other consequence of a data breach may include reputational damage, loss of customers, loss of sales, damage to partner or peer relationships, legal costs, fines and insurance claims.

The Benefits of PCI DSS Compliance

PCI DSS Compliance reduces the risk of payment card fraud and ensures merchants protect their customers and their customer's sensitive data.

PCI DSS Compliance means that customers and partners can trust the merchants to appropriately handle their payment card information; customer confidence in the merchant is increased. A confident customer is more likely to use and to return to that merchant's services and is more likely to recommend their services to others.

PCI DSS Compliance enhances a merchant's reputation amongst their peers, with acquirers and with the card brands.

PCI DSS is a data security standard and compliance also means that the merchant systems are more secure, that security risks outside of those specific to cardholder data are also reduced, and that other information security regulations and standards can be more easily complied with.

Merchants may use PCI DSS as the basis for a comprehensive Information Security Management System for their organisation.