Payment Card Industry Data Security Standards (PCI DSS) Frequently Asked Questions

While the Payment Card Industry Data Security Standard, commonly referred to as PCI or PCI DSS, has been in existence for many years, many merchants still have questions about what it is and what it requires. In addition, the explosion of new technologies and business models that have been recently introduced bring new concerns about protecting customer data. Protecting sensitive payment data is a requirement for all merchants, large and small. This paper is intended to answer some important questions about what the PCI DSS requires and how merchants can comply.

What is the PCI DSS and why do I have to comply?

The PCI DSS is a set of data security requirements that are mandated by the major card brands. All merchants, and any entity that stores, processes, or transmits cardholder data on behalf of a merchant, must comply with the PCI DSS. The PCI DSS contains 12 high-level requirements, each with a set of sub-requirements, totaling more than 350 components.

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 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 all personnel

Figure 1: *Payment Card Industry (PCI) Data Security Standard, v3.1 © 2006-2015 PCI Security Standards Council, LLC. All Rights Reserved.*

Compliance with the PCI DSS is mandatory for all merchants. Failure to comply can result in fines, fees and assessments passed through the acquirer to the merchant.

The PCI DSS is concerned with the protection of "cardholder data." What is considered "cardholder data?"

Cardholder Data is defined as the Primary Account Number (PAN) alone. Storing, transmitting or processing a single PAN obligates a company to comply with the PCI DSS. The PAN is the 15-19 digit number that is embossed on the front of the card. Cardholder name, expiration date, and service code can also be considered Cardholder Data under certain circumstances. This data is stored on the magnetic stripe of the credit or debit card, along with other sensitive authentication data. Sensitive

authentication data allows the payment processor and the bank that issued the card to validate the card that is being used. If data thieves are able to access this data, they can create counterfeit cards and initiate fraudulent transactions.

How do I validate compliance with the PCI DSS?

The manner in which a merchant must validate compliance with the PCI DSS is determined by how many transactions that merchant processes on an annual basis. Large merchants must undergo an onsite assessment by a Qualified Security Assessor (QSA), a security professional that has been vetted by the Payment Card Industry Security Standards Council (PCI SSC). Smaller merchants can validate using a Self-Assessment Questionnaire (SAQ). The merchant levels are depicted in the table below.

Level	Transaction Volume	Validation Method
1	More than 6 Million transactions annually of any one card brand	Annual Onsite assessment and quarterly vulnerability scans*
2	Between 1-6 M transactions annually through any acceptance channel	Annual Self-Assessment Questionnaire and quarterly vulnerability scans*
3	20,000 to 1M eCommerce transactions annually	Annual Self-Assessment Questionnaire and quarterly vulnerability scans*
4	Merchants processing less than 20,000 eCommerce transactions and all other merchants processing less than 1 M transactions annually	Annual Self-Assessment Questionnaire and quarterly vulnerability scans*

Figure 2: Merchant Levels and Validation Requirements

**Vulnerability scans may not be applicable depending on the architecture of the individual merchant's environment.*

There are many Self-Assessment Questionnaires. Which one do I have to complete in order to validate compliance?

The appropriate SAQ is determined according to the way in which a merchant accepts and interacts with Cardholder Data. If a merchant is using a hosted payment page, for instance, and has no electronic storage of Cardholder Data, then according to the most recent version of the PCI DSS, that merchant would validate compliance using the "SAQ A." On the other end of the spectrum, if a merchant uses its own systems to store, process, or transmit Cardholder Data and does have some electronic storage of Cardholder Data, it would validate compliance using the "SAQ D-Merchant." It should be noted that the PCI SSC occasionally introduces new Self-Assessment Questionnaires. In that case, a merchant may have to validate differently than it had done in previous years.

Are there services that can assist merchants in filling out the SAQ?

There are a number of companies that provide assistance in filling out SAQ documentation and can provide the quarterly vulnerability scans if they are required. ProPay has partnered with ControlScan to assist its merchants in achieving and validating compliance. For more information about that service, merchants can visit www.controlscan.com/propay. There is a $75 annual fee for the service. Merchants that are interested in using the ControlScan service can email compliance@propay.com to enroll.

Once a merchant validates compliance, what is required?

After completing the validation process, merchants should send their documentation to ProPay. If a merchant is using ControlScan, its validation is automatically recorded and the documentation is made available to ProPay through ControlScan's portal. On a quarterly basis, ProPay must report to the card brands on the compliance of its merchants. Additionally, if vulnerability scans are required, they must be done on a quarterly basis. A merchant that does not submit compliant scans on a quarterly basis is not compliant with the PCI DSS.

If a merchant outsources the storage, processing, and transmission of cardholder data to a third party, does that merchant still have to validate compliance with the PCI DSS?

Yes. A merchant cannot outsource the requirement to achieve and validate compliance. The use of a compliant third party can significantly reduce the scope of the compliance work required by the merchant, but the merchant must still achieve and validate compliance with the PCI DSS. In addition, the merchant can only be considered compliant if the service provider being used is PCI DSS compliant, as well. Merchants are required by the PCI DSS to contractually obligate the service provider to be PCI DSS compliant and to demonstrate that compliance through an Attestation of Compliance (AOC) to the merchant. Merchants must also notify their acquirer of the service provider being used, as the service provider may be required to register with the card brands. A list of compliant service providers can be found at http://www.visa.com/splisting/searchGrsp.do.