



PCI DSS FREQUENTLY ASKED QUESTIONS

Q: Are there any merchants that do not have to follow the PCI DSS requirements?

A: No, all merchants must follow and practice PCI requirements.

Q: How does the merchant know which one of the four levels they would be categorized? Is there a tool that captures the 4 merchant level definitions?

A: All merchants will fall into one of the four merchant levels based on annual transaction volume:

Level 4 (less than 20,000 transactions) – PCI Self-Assessment Questionnaire not required BUT strongly recommended by Global Payments

Level 3 (20,000 to 1,000,000 transactions) – PCI Self-Assessment Questionnaire required, Qualified Security Assessor recommended

Level 2 (1,000,000 to 6,000,000 transactions) – PCI Self-Assessment Questionnaire required, Qualified Security Assessor recommended

Level 1 (over 6,000,000 transactions) – Qualified Security Assessor Audit required

Q: Should a sales rep always include the PCI discussion as part of the application process?

A: Yes.

Q: What is the sales rep ultimately responsible for when facilitating a new contract?

- A:*
- 1. Obtain the software application and version number for the merchants' POS,*
 - 2. Complete the CARD DATA STORED fields in MEA,*
 - 3. Include the POS application name and version number in the PRIMARY CAP/VAR field,*
 - 4. If necessary, perform post enrollment changes*

Q: What does the credit analyst review when underwriting a new application?

A: The analyst will cross check and make sure the data entered on the contract matches exactly the information entered into MEA.

Q: What if it's a new merchant accepting credit cards for the first time, how do we know what level the merchant will be for PCI DSS?

A: Each and every merchant, with the help of their sales rep, can project an average ticket and a potential volume which determines the number of annual transactions (See the merchant level definitions chart in the PCI Quick Reference Guide)

Q: How do I calculate the number of transactions? Is it just for credit card transactions or all transactions that a merchant processes?

A: All major credit/debit card transactions apply to the number of transactions calculation. The number of transactions can be calculated when dividing the annual volume by the average ticket size.

Q: What can a sales rep use to explain and/or present PCI DSS to a merchant?

A: The PCI SSC Quick Guide.

SECURITY ASSESSMENT

Q: What does SAQ stand for; what does it really mean?

A: Security Assessment Questionnaire; the merchant can complete it by going to <https://www.pcisecuritystandards.org/saq/instructions.shtml>

Q: What are the merchants' responsibilities once they have completed the SAQ or QSA?

A: Keep a copy of the paperwork on file with their business AND be sure to accurately complete the PCI DSS section of the Application

Q: If a merchant is required to perform a Security Assessment (SAQ or QSA) but has not completed it at the time the contract is signed, can I still submit the merchant contract to Credit?

A: No, the SAQ or QSA must be completed prior to signing the Application.

Q: If a merchant has a terminal, do they have to perform a Security Assessment?

A: Merchants using stand alone regular credit card terminals/machines are not required to get assessed but it is highly recommended.

Q: How often do merchants need to perform the Security Assessment?

A: Annually.

Q: Does the merchant have to perform the SAQ or QSA if the third party vendor is already certified and compliant?

A: Yes, see the merchant level definitions chart in the PCI Quick Reference Guide

Q: Is there a QSA that Global Payments recommends to merchants?

A: Yes, Trustwave is strongly recommended <https://www.trustwave.com/>

Q: If the merchant does not want to use Trustwave as the QSA, who can the merchant use to be assessed?

A: See List of Qualified Security Assessors https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf

DATA STORAGE

Q: What does...Are you using a "dial up" terminal mean and what should they do for PCI DSS?

A: The credit card terminal is processing with a telephone line. Merchants using stand alone regular credit card terminals are not required to get assessed but it is highly recommended.

Q: Where can you go to see common POS situations that might come into play while completing the Contract and MEA?

A: See "Common Scenarios" in the Global Payments PCI Quick Reference Guide.

Q: Do all third party applications store cardholder data?

A: Yes – In PCI terms, "Stored only" implies receive, pass, transmit, or store.

Q: In the case of Global Transport, why is cardholder data stored at the merchant?

A: Card Data "Stored" = identifies if the merchant transmits, stores, or receives cardholder's data.

Global Transport VT is a Global Payments Class A Web Based Product and the transactions are directly routed through our (Global's) host to and from the merchant.

Q: If PC Charge software (example) is "storing" transactions on the PC, how would we complete the PCI DSS section of the Global Payment's Contract?

A: PC Charge is a Third Party Class B Application; if a Third Party Class B Application resides entirely on the PC (and is not web based) then you can check the box on the application "Merchant & Third Party" rather than just the "third party" selection.

Q: What if the merchant is using a foreign front end processor?

A: All of the same rules apply for a merchant using a foreign front end such as Visanet (Vital) or Envoy.

Q: What are the steps if an existing merchant updates their software or obtains a new software application?

*A: **Update the changes in MAS***

COMPLIANCE/CERTIFICATION

Q: What if a third party application is not in our database but is in the compliant list provided by Visa?

A: The software application must be either certified or re-certified to Global Payments.

Q: What if an application is not on either the Visa compliant list or the Global Payments database?

A: The merchant should not use the payment application OR must wait until the application is certified and compliant with Visa as well as Global Payments.

Q: If an application is in the Global Payments database, are we sure it is compliant?

A: Yes.

Q: What does Date of compliance & Date of last scan mean?

A: The date the merchant completed the SAQ or QSA & the last time the merchant was assessed if they previously performed the SAQ or QSA.

GLOBAL PAYMENTS

Q: Is Global the only processor that has to abide by the PCI rules?

A: No, ALL Payment Processors (acquirers) must follow ALL PCI requirements.

Q: What category do most of Global Payment's direct merchants fall into?

A: Most common merchants will most likely fall into the Level 3 or Level 4 categories.

Q: What is the cost for a QSA or SAQ? Does Global Payments charge the merchant for PCI compliance?

A: The SAQ (Self Assessment Questionnaire) has no cost associated with it. If the merchant elects a QSA (Qualified Security Assessor) to perform the security assessment, then the QSA could potentially charge the merchant for the service, which is clearly at the discretion of the QSA. Global Payments does not charge merchants for PCI compliance.