Payment Card Industry Data Security Standard (PCI DSS)

Payment Card Industry Data Security Standard (PCI DSS) is intended for **_ALL_ _who involved in payment processing_**, that includes merchants, issuing banks, Service provers or who affects the card holder data security regardless of their size or transaction volume.

Typically, smaller merchants often have simpler environments, with limited amounts of cardholder data and fewer applications/systems that needs protection.

Individual payments brands and acquiring banks determines whether small merchants required to validate PCI compliance.

For questions related to your compliance validation and reporting requirements, please contact your acquirer (merchant bank) or payment brand you do business with, as applicable.

Payment Card Industry Data Security Standard (PCI DSS)

Merchant: For the purposes of the PCI Data Security Standard (PCI DSS) Council definition, a merchant is defined as **any entity that accepts payment cards bearing the logos of any of the six members of PCI SSC (American Express, Discover, JCB, MasterCard, UnionPay or Visa) as payment for goods and/or services**.

Service providers: For the purposes of the PCI Data Security Standard (PCI DSS) Council definition, service provider is a: "**Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity**".

VISA's Compliance validation Requirements for **Merchants**

Total # of Transactions Annually	Levels	Requirements *(What you have to do)*	PCI Compliance status Validation *(Mandatory / Optional)*	Who completes the assessments	Document
Over 6 Million or Compromised / Breached merchant	1	➢ **Every year:** ❑ File a Report on Compliance ("ROC") by Qualified Security Assessor ("QSA")" or Internal Auditor if signed by officer of the company. *Visa recommend the internal auditor obtain the PCI SSC Internal Security Assessor ("ISA") certification.* ❑ Annual On-site Assessment. ❑ Submit an Attestation of Compliance ("AOC") Form ➢ **Every quarter:** ❑ Conduct a quarterly network scan by an Approved Scan Vendor ("ASV")	Mandatory since Sep 2010	1. Qualified Security Assessor - QSA (Annual On-site Assessment)/Qualified Internal Resources (e.g ISA). 2. Approved Scanning Vendor (ASV) for scanning reports	1. ROC template will be provided by your QSA/Qualified Internal resource 2. ASV provides scanning reports 3. Attestation of Compliance Form
1 - 6 Million	2		Mandatory Since Sep 2010	1. Qualified Internal Assessor/Qualified Internal Resources (e.g ISA).(engage QSA if necessary). 2. Approved Scanning Vendor (ASV) for scanning reports	1. SAQ (Look at the SAQ requirements to select right SAQ form to be completed) 2. ASV provides scanning reports 3. Attestation of Compliance Form
20,000 to 1 Million Visa e-Commerce	3	➢ **Every year:** ❑ Complete a Self-Assessment Questionnaire ("SAQ"). ❑ Submit an Attestation of Compliance ("AOC") Form. ➢ **Every quarter:** ❑ Conduct a quarterly network scan by an Approved Scan Vendor ("ASV") (Mandatory for all level other than level 4, for level 4 do this if applicable*) *Note: Compliance validation requirements are set by your acquiring bank for level 4 Merchants.	Mandatory (compliance date is set by your Acquiring Bank)	1. Qualified Internal Assessor/Qualified Internal Resources (e.g ISA). 2. Approved Scanning Vendor (ASV) for scanning reports	1. SAQ (Look at the SAQ requirements to select right SAQ form to be completed) 2. ASV provides scanning reports 3. Attestation of Compliance Form
Less than 20,000 Visa E-commerce	4		Mandatory (compliance date is set by your Acquiring Bank)	1. Qualified Internal Assessor/Qualified Internal Resources (e.g ISA). 2. Approved Scanning Vendor (ASV) for scanning reports	1. SAQ (Look at the SAQ requirements to select right SAQ form to be completed) 2. ASV provides scanning reports 3. Attestation of Compliance Form
Up to 1 Million but not specific to E-commerce category above	4		Mandatory (compliance date is set by your Acquiring Bank)	1. Qualified Internal Assessor/Qualified Internal Resources (e.g ISA). 2. Approved Scanning Vendor (ASV) for scanning reports	1. SAQ (Look at the SAQ requirements to select right SAQ form to be completed) 2. ASV provides scanning reports 3. Attestation of Compliance Form

Total # of Transactions Annually	Levels	Requirements *(What you have to do)*	PCI Compliance status *(Mandatory / Optional)*	Who completes the assessments	Document
VisaNet Processor or any service provider that stores/transmit/process **over 300,000** transaction count	1	➤ **Every year:** ❑ File a Report on Compliance ("ROC") by Qualified Security Assessor ("QSA")" ❑ Annual On-site Assessment. ❑ Submit an Attestation of Compliance ("AOC") Form ➤ **Every quarter:** ❑ Conduct a quarterly network scan by an Approved Scan Vendor ("ASV")	Mandatory since Sep 2010	1. Qualified Security Assessor - QSA (Annual On-site Assessment). 2. Approved Scanning Vendor(ASV)	1. Annual on-site PCI data security assessment (ROC) 2. Submit an executed attestation of compliance (AOC), signed by both the service provider and the qualified security assessor (QSA) to Visa. 3. ASV provides scanning reports
Any service provider that stores/transmit/process **under 300,000** transaction count	2	➤ **Every year:** ➤ File a Report on Compliance ("ROC") by Qualified Security Assessor ("QSA")" or Internal Auditor if signed by officer of the company. *Visa recommend the internal auditor obtain the PCI SSC Internal Security Assessor ("ISA") certification.* ➤ Submit an Attestation of Compliance ("AOC") Form **Every quarter:** ➤ Conduct a quarterly network scan by an Approved Scan Vendor ("ASV")	Mandatory Since Sep 2010	1. Qualified Security Assessor - QSA /Qualified Internal Resources (e.g ISA). 2. Approved Scanning Vendor(ASV)	1. Annual on-site PCI data security assessment **(SAQ-D)** Or 1. Submit an executed attestation of compliance (AOC), signed by qualified security assessor (QSA) to Visa. 2. ASV provides scanning reports

Note: Merchant level identification is based on the corporate entity's total volume of VISA transactions (inclusive of credit, debit and prepaid) meeting the transaction thresholds in one country or with one acquirer per year. Volume from independently-owned and operated merchant locations (e.g., franchisee, licensee) may be excluded if it is not processed by the corporate entity.

4

Total # of Transactions Annually	Levels	Requirements *(What you have to do)*	PCI Compliance status *(Mandatory / Optional)*	Who completes the assessments	Document
Over 6 Million or Compromised / Breached merchant **or** Any Level 1 criteria of Visa	1	➢ **Every year:** ❑ File a Report on Compliance ("ROC") by Qualified Security Assessor ("QSA")" or Internal Auditor if signed by officer of the company. MasterCard recommend the internal auditor obtain the PCI SSC Internal Security Assessor ("ISA") certification. ❑ Annual On-site Assessment. ❑ Submit an Attestation of Compliance ("AOC") Form ➢ **Every quarter:** ❑ Conduct a quarterly network scan by an Approved Scan Vendor ("ASV")	Mandatory	1. Qualified Security Assessor - QSA (Annual On-site Assessment)/Qualified Internal Resources (e.g ISA). 2. Approved Scanning Vendor (ASV) for scanning reports	1. ROC template will be provided by your QSA/Qualified Internal resource 2. ASV provides scanning reports 3. Attestation of Compliance Form
1 - 6 Million **or** Any Level 2 criteria of Visa	2	➢ **Every year:** ❑ Complete a Self-Assessment Questionnaire ("SAQ"). ❑ Submit an Attestation of Compliance ("AOC") Form. ➢ **Every quarter:** ❑ Conduct a quarterly network scan by an Approved Scan Vendor ("ASV") *Note: Compliance date is set by your acquiring bank for level 4 Merchants.*	Mandatory	1. Qualified Internal Assessor/Qualified Internal Resources (e.g ISA).*(Level 2 merchants completing SAQ A, SAQ A-EP or SAQ D must additionally engage a PCI SSC-approved QSA or PCI SSC-certified ISA for compliance validation).* 2. Approved Scanning Vendor (ASV) for scanning reports	1. SAQ (Look at the SAQ requirements to select right SAQ form to be completed) 2. ASV provides scanning reports 3. Attestation of Compliance Form
20,000 to 1 Million MasterCard and Maestro e-Commerce but less than 1 Million total **or** Any Level 3 criteria of Visa	3		Mandatory	1. Qualified Internal Assessor/Qualified Internal Resources (e.g ISA). 2. Approved Scanning Vendor (ASV) for scanning reports	1. SAQ (Look at the SAQ requirements to select right SAQ form to be completed) 2. ASV provides scanning reports 3. Attestation of Compliance Form
All others who not fall under above category **or** Any Level 4 criteria of Visa	4		Mandatory	1. Qualified Internal Assessor/Qualified Internal Resources (e.g ISA). 2. Approved Scanning Vendor (ASV) for scanning reports	1. SAQ (Look at the SAQ requirements to select right SAQ form to be completed) 2. ASV provides scanning reports 3. Attestation of Compliance Form

Note: Merchant level identification is based on the corporate entity's total volume of total combined Mastercard and Maestro transactions (inclusive of credit, debit and prepaid) annualy

MasterCard's Compliance validation Requirements for Service Providers

Total # of Transactions Annually	Levels	Requirements (What you have to do)	PCI Compliance status (Mandatory / Optional)	Who completes the assessments	Document
All Third Party Processors (TPP) **or** Any Data Storing Entities (DSE) that stores/transmit/process **over 300,000** transaction (total combined Mastercard and Maestro transactions annually)	1	➢ **Every year:** ❑ File a Report on Compliance ("ROC") by Qualified Security Assessor ("QSA")" ❑ Annual On-site Assessment. ❑ Submit an Attestation of Compliance ("AOC") Form ➢ **Every quarter:** ❑ Conduct a quarterly network scan by an Approved Scan Vendor ("ASV")	Mandatory since Sep 2010	1. Qualified Security Assessor - QSA (Annual On-site Assessment). 2. Approved Scanning Vendor(ASV)	1. Annual on-site PCI data security assessment (ROC) by qualified security assessor (QSA). 2. ASV provides scanning reports
Any Data Storing Entities (DSE) that stores/transmit/process **300,000 or less** transaction (total combined Mastercard and Maestro transactions annually)	2	➢ **Every year:** ❑ File a Report on Compliance ("ROC") by Qualified Security Assessor ("QSA")" or Internal Auditor if signed by officer of the company. _Visa recommend the internal auditor obtain the PCI SSC Internal Security Assessor ("ISA") certification._ ❑ Submit an Attestation of Compliance ("AOC") Form ➢ **Every quarter:** ❑ Conduct a quarterly network scan by an Approved Scan Vendor ("ASV")	Mandatory Since Sep 2010	1. QSA/Qualified Internal Resources (e.g ISA). 2. Approved Scanning Vendor(ASV)	1. Annual on-site PCI data security assessment (SAQ-D) by QSA/ISA. 2. ASV provides scanning reports

Note: Merchant level identification is based on the corporate entity's total volume of VISA transactions (inclusive of credit, debit and prepaid) meeting the transaction thresholds in one country or with one acquirer per year. Volume from independently-owned and operated merchant locations (e.g., franchisee, licensee) may be excluded if it is not processed by the corporate entity.

Total # of Transactions Annually	Levels	Requirements *(What you have to do)*	PCI Compliance status *(Mandatory / Optional)*	Who conducts the Assessment	Documents
Over 2.5 Million	1	➢ **Every year:** ❑ File a Report on Compliance ("ROC") by Qualified Security Assessor ("QSA")" or Internal Auditor if signed by officer of the company. AMEX recommend the internal auditor obtain the PCI SSC Internal Security Assessor ("ISA") certification. ❑ Annual On-site Assessment. ❑ Submit an Attestation of Compliance ("AOC") Form ➢ **Every quarter:** ❑ Conduct a quarterly network scan by an Approved Scan Vendor ("ASV")	Mandatory for Merchants and Service providers	1. Qualified Security Assessor - QSA (Annual On-site Assessment)/Qualified Internal Resources (e.g ISA). 2. Approved Scanning Vendor (ASV) for scanning reports 3. External Network Vulnerability Scan	1. Report on Compliance (ROC) 2. Attestation of Compliance (AOC). 3. Other acceptable documentation: American Express STEP Attestation
Between 50,000 and 2.5 Million	2	➢ **Every year:** ❑ Complete a Self-Assessment Questionnaire ("SAQ"). ❑ Submit an Attestation of Compliance ("AOC") Form. ➢ **Every quarter:** ❑ Conduct a quarterly network scan by an Approved Scan Vendor ("ASV").	Mandatory for Merchants and Service provider	1. Qualified Internal Resources (e.g ISA) for Annual Self assessment. 2. Approved Scanning Vendor (ASV) for scanning reports. 3. External Network Vulnerability Scan	1. SAQ (Look at the SAQ requirements to select right SAQ form to be completed) 2. ASV Scan Report Attestation of Scan Compliance (AOSC) 3. Other acceptable documentation: Report on Compliance Attestation of Compliance (ROC AOC) American Express STEP Attestation
Between 10,000 and 50,000	3		If required by American Express, otherwise optional	1. Qualified Internal Resources (e.g ISA) for Annual Self assessment. 2. Approved Scanning Vendor (ASV) for scanning reports. 3. External Network Vulnerability Scan	1. SAQ (Look at the SAQ requirements to select right SAQ form to be completed) 2. ASV Scan Report Attestation of Scan Compliance (AOSC) 3. Other acceptable documentation: Report on Compliance Attestation of Compliance (ROC AOC) American Express STEP Attestation
Less than 10,000	4		If required by American Express, otherwise optional	1. Qualified Internal Resources (e.g ISA) for Annual Self assessment. 2. Approved Scanning Vendor (ASV) for scanning reports.	1. SAQ (Look at the SAQ requirements to select right SAQ form to be completed) 2. ASV Scan Report Attestation of Scan Compliance (AOSC) 3. Other acceptable documentation: Report on Compliance Attestation of Compliance (ROC AOC) American Express STEP Attestation

Note: Merchant level identification is based on the corporate entity's total volume of AMEX transactions (inclusive of credit, debit and prepaid) meeting the transaction thresholds in one country or with one acquirer per year.

DISCOVER's Compliance validation Requirements for Merchants

Total # of Transactions Annually	Levels	Requirements *(What you have to do)*	PCI Compliance status *(Mandatory / Optional)*	Who conducts the Assessment	Documents
Over 6 Million card transaction on Discover Network Or Any merchant that Discover, in its sole discretion, determines should meet the Level 1 compliance validation and reporting requirements. Or All merchants required by another payment brand or acquirer to validate and report their compliance as a Level 1 merchant.	1	➤ **Every year:** ❑ File a Report on Compliance ("ROC") by Qualified Security Assessor ("QSA")" or Internal Security Assessor (ISA) if signed by officer of the company. ❑ Annual On-site Assessment. ❑ Submit an Attestation of Compliance ("AOC") Form ➤ **Every quarter:** ❑ Conduct a quarterly network scan by an Approved Scan Vendor ("ASV")	Mandatory for Merchants	1. Qualified Security Assessor - QSA Qualified Internal Resources (e.g ISA). - For Annual On-site Assessment 2. Approved Scanning Vendor (ASV) for scanning reports 3. External Network Vulnerability Scan	1. Attestation of Compliance (AOC) from Report on Compliance (ROC) 2. Submission of scan results **not** required Note: Discover reserves the right to request and receive a copy of a Merchant's full Report on Compliance (ROC) or Self-Assessment Questionnaire (SAQ) at any time.
Between 1 Million and 6 Million card transactions on the Discover Network	2	➤ **Every year:** ❑ Complete a Self-Assessment Questionnaire ("SAQ"). ❑ Submit an Attestation of Compliance ("AOC") Form. ➤ **Every quarter:** ❑ Conduct a quarterly network scan by an Approved Scan Vendor ("ASV"). Note: Discover reserves the right to request and receive a copy of a Merchant's full Report on Compliance (ROC) or Self-Assessment Questionnaire (SAQ) at any time.	Mandatory for Merchants	1. Qualified Internal Resources (e.g ISA) for Annual Self assessment. 2. Approved Scanning Vendor (ASV) for scanning reports. 3. External Network Vulnerability Scan	1. Attestation of Compliance (AOC) from SAQ. For SAQ (Look at the SAQ requirements to select right SAQ form to be completed) 2. Submission of scan results **not** required
All other merchants	3		Mandatory for Merchants	1. Qualified Internal Resources (e.g ISA) for Annual Self assessment. 2. Approved Scanning Vendor (ASV) for scanning reports. 3. External Network Vulnerability Scan	1. Attestation of Compliance (AOC) from SAQ. For SAQ (Look at the SAQ requirements to select right SAQ form to be completed) 2. Submission of scan results **not** required

Note: Merchant level identification is based on the corporate entity's total volume of DISCOVER transactions (inclusive of credit, debit and prepaid) meeting the transaction thresholds in one country or with one acquirer per year.

DISCOVER's Compliance validation Requirements for Service Providers

Total # of Transactions Annually	Levels	Requirements *(What you have to do)*	PCI Compliance status *(Mandatory / Optional)*	Who conducts the Assessment	Documents
All Service Providers that store, process and/or transmit **over 300,000** Discover card transactions per year	1	➢ **Every year:** ❑ File a Report on Compliance ("ROC") by Qualified Security Assessor ("QSA")" ❑ Annual On-site Assessment. ❑ Submit an Attestation of Compliance ("AOC") Form ➢ **Every quarter:** ❑ Conduct a quarterly network scan by an Approved Scan Vendor ("ASV")	Mandatory for Service providers	1. Qualified Security Assessor - QSA Qualified Internal Resources (e.g ISA). - For Annual On-site Assessment 2. Approved Scanning Vendor (ASV) for scanning reports	1. Attestation of Compliance (AOC) from Report on Compliance (ROC) 2. Submission of scan results **not** required Note: Discover reserves the right to request and receive a copy of a Merchant's full Report on Compliance (ROC) or Self-Assessment Questionnaire (SAQ) at any time.
All Service Providers that store, process and/or transmit **less than 300,000** Discover card transactions per year	2	**Every year:** ❑ Complete a Self-Assessment Questionnaire ("SAQ"). Service Providers that perform a self-assessment are required to complete PCI DSS Self-Assessment Questionnaire D and submit the Service Provider Version of the Attestation of Compliance. ❑ Submit an Attestation of Compliance ("AOC") Form. **Every quarter:** ❑ Conduct a quarterly network scan by an Approved Scan Vendor ("ASV").	Mandatory for Service providers	1. Qualified Internal Resources (e.g ISA) for Annual Self assessment. 2. Approved Scanning Vendor (ASV) for scanning reports.	1. Attestation of Compliance (AOC) from SAQ 2. Submission of scan results **not** required Note: Discover reserves the right to request and receive a copy of a Merchant's full Report on Compliance (ROC) or Self-Assessment Questionnaire (SAQ) at any time.

Note: Merchant level identification is based on the corporate entity's total volume of DISCOVER transactions (inclusive of credit, debit and prepaid) meeting the transaction thresholds in one country or with one acquirer per year.

JCB's Compliance validation Requirements for Merchants / Service Providers

Total # of Transactions Annually	Levels	Requirements *(What you have to do)*	PCI Compliance status *(Mandatory / Optional)*	Who conducts the Assessment	Documents
Merchants (Not including IPSPs) Attended Transaction, Cardmember Operated Terminal Transaction OR E-commerce Transaction, MO/TO Transaction, Phone Call Service Transaction (either IPSPs or not). **More than 1 Million** transaction annually Any IPSPs with any # of transactions.	1	➤ **Every year:** ❑ File a Report on Compliance ("ROC") by Qualified Security Assessor ("QSA")" or Internal Security Assessor (ISA) if signed by officer of the company. ❑ Submit an Attestation of Compliance ("AOC") Form ➤ **Every quarter:** ❑ Conduct a quarterly network scan by an Approved Scan Vendor ("ASV")	Mandatory for Merchants (On and after April 1, 2020 for attended transaction category merchants and April1, 2018 for e-commerce, MO/TO type merchants)	1. Qualified Security Assessor - QSA Qualified Internal Resources (e.g ISA). - For Annual On-site Assessment 2. Approved Scanning Vendor (ASV) for scanning reports 3. External Network Vulnerability Scan Note: A PCI SSC Approved Scanning Vendor (ASV) performs a remote network security scan of your network and web applications to evaluate system vulnerabilities and misconfigurations to attempted intrusions over the Internet.	1. Attestation of Compliance (AOC) from Report on Compliance (ROC) 2. ASV scanning report
Merchants (Not including IPSPs) Attended Transaction, Cardmember Operated Terminal Transaction OR E-commerce Transaction, MO/TO Transaction, Phone Call Service Transaction (either IPSPs or not). **Less than 1 Million** transaction annually	2	➤ **Every year:** ❑ Complete a Self-Assessment Questionnaire ("SAQ"). ❑ Submit an Attestation of Compliance ("AOC") Form. ➤ **Every quarter:** ❑ Conduct a quarterly network scan by an Approved Scan Vendor ("ASV").	Mandatory for Merchants (On and after April 1, 2020 for attended transaction category merchants and April1, 2018 for e-commerce, MO/TO type merchants)	1. Qualified Internal Resources (e.g ISA) for Annual Self assessment. 2. Approved Scanning Vendor (ASV) for scanning reports. 3. External Network Vulnerability Scan Note: A PCI SSC Approved Scanning Vendor (ASV) performs a remote network security scan of your network and web applications to evaluate system vulnerabilities and misconfigurations to attempted intrusions over the Internet.	1. Attestation of Compliance (AOC) from SAQ. For SAQ (Look at the SAQ requirements to select right SAQ form to be completed) 1. ASV scanning report

Note: Merchant level identification is based on the corporate entity's total volume of DISCOVER transactions (inclusive of credit, debit and prepaid) meeting the transaction thresholds in one country or with one acquirer per year.

Which SAQ Best Applies to My Environment?

SAQ SELECTION INSTRUCTIONS

- ✔ To determine the applicable SAQs, follow the path(s) for EACH channel.
- ✔ If the answer to the question is "YES," check the box for each applicable SAQ that follows.
- ✔ Merchants with more than one channel should consult with their acquirer about how to validate compliance.
- ✔ Merchants must meet all eligibility criteria for any applicable SAQ.

© 2017 PCI Security Standards Council LLC.

The intent of this document is to provide supplemental information, which does not replace or supersede PCI SSC Security Standards or their supporting documents.

www.pcisecuritystandards.org

11