## Payment Card Industry Data Security Standard (PCI DSS)

Payment Card Industry Data Security Standard (PCI DSS) is intended for <u>ALL who</u> <u>involved in payment processing</u>, 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".

Total # of Transactions Annually	Levels	Requirements (What you have to do)	PCI Compliance status Validation(Mandato ry/Optional)	Who completes the assessments	Document
Over 6 Million or Compromised / Breached merchant	1	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	<ol> <li>Qualified Security Assessor - QSA (Annual On-site Assessment)/Qualified Internal Resources (e.g ISA).</li> <li>Approved Scanning Vendor (ASV) for scanning reports</li> </ol>	<ol> <li>ROC template will be provided by your QSA/Qualified Internal resource</li> <li>ASV provides scanning reports</li> <li>Attestation of Compliance Form</li> </ol>
1 - 6 Million	2	2/0/3/	Mandatory Since Sep 2010	<ol> <li>Qualified Internal Assessor/Qualified Internal Resources (e.g ISA).(engage QSA if necessary).</li> <li>Approved Scanning Vendor (ASV) for scanning reports</li> </ol>	<ol> <li>SAQ (Look at the <u>SAQ requirements</u> to select right SAQ form to be completed)</li> <li>ASV provides scanning reports</li> <li>Attestation of Compliance Form</li> </ol>
20,000 to 1 Million Visa e-Commerce	3	<ul> <li>➤ Every year:</li> <li>□ Complete a Self-Assessment Questionnaire ("SAQ").</li> <li>□ Submit an Attestation of Compliance ("AOC") Form.</li> <li>➤ Every quarter:</li> </ul>	Mandatory (compliance date is set by your Acquiring Bank)	<ol> <li>Qualified Internal Assessor/Qualified Internal Resources (e.g ISA).</li> <li>Approved Scanning Vendor (ASV) for scanning reports</li> </ol>	<ol> <li>SAQ (Look at the <u>SAQ requirements</u> to select right SAQ form to be completed)</li> <li>ASV provides scanning reports</li> <li>Attestation of Compliance Form</li> </ol>
Less than 20,000 Visa E-commerce	4	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*)	Mandatory (compliance date is set by your Acquiring Bank)	<ol> <li>Qualified Internal Assessor/Qualified Internal Resources (e.g ISA).</li> <li>Approved Scanning Vendor (ASV) for</li> </ol>	SAQ (Look at the <u>SAQ requirements</u> to select right SAQ form to be completed)     ASV provides scanning reports

E-commerce Up to 1 Million but not

category above

specific to E-commerce

4

\*Note: Compliance validation requirements are set by your acquiring bank for level 4 Merchants.

Acquiring Bank) Mandatory (compliance date is set by your

Acquiring Bank)

scanning reports 1. Qualified Internal Assessor/Qualified Internal Resources (e.g ISA).

2. Approved Scanning Vendor (ASV) for

3. Attestation of Compliance Form 1. SAQ (Look at the SAQ requirements to select right SAQ form to be completed) 2. ASV provides scanning reports

**Attestation of Compliance Form** 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

VI3	A's Compliance validation Requirements for	Service Providers	Copyright & 2023 Global Risk In	Management Services Group L.L.C.   All Rights Reserved.
Levels	Requirements (What you have to do)	PCI Compliance status (Mandatory / Optional)	Who completes the assessments	Document
1		Mandatory since Sep 2010	<ol> <li>Qualified Security         Assessor - QSA         (Annual On-site         Assessment).</li> <li>Approved Scanning         Vendor(ASV)</li> </ol>	<ol> <li>Annual on-site PCI data security assessment (ROC)</li> <li>Submit an executed attestation of compliance (AOC), signed by both the service provider and the qualified security assessor (QSA) to Visa.</li> <li>ASV provides scanning reports</li> </ol>
2	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	<ol> <li>Qualified Security         Assessor - QSA         /Qualified Internal         Resources (e.g ISA).</li> <li>Approved Scanning         Vendor(ASV)</li> </ol>	<ol> <li>Annual on-site PCI data security assessment (SAQ-D)</li> <li>Or</li> <li>Submit an executed attestation of compliance (AOC), signed by qualified security assessor (QSA) to Visa.</li> <li>ASV provides scanning reports</li> </ol>
ti	1 2	File a Report on Compliance ("ROC") by Qualified Security Assessor ("QSA")"  Annual On-site Assessment.  Submit an Attestation of Compliance ("AOC") Form  Fivery quarter:  Conduct a quarterly network scan by an Approved Scan Vendor ("ASV")  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 ("QSA")" or Submit an Attestation of Compliance ("AOC") Form  Every quarter:  Conduct a quarterly network scan by an Approved Scan Vendor ("ASV")	File a Report on Compliance ("ROC") by Qualified Security Assessor ("QSA")"   Annual On-site Assessment.   Submit an Attestation of Compliance ("AOC") Form   Mandatory since Sep 2010   File a Report on Compliance ("ROC") by Qualified Security Assessor ("QSA")"   Annual On-site Assessment.   Conduct a quarterly network scan by an Approved Scan Vendor ("ASV")   Mandatory since Sep 2010   File a Report on Compliance ("ROC") by Qualified Security Assessor ("QSA")" or Internal Auditor if signed by officer of the company. **Supermoment the internal outlion obtain the PCISSC Internal Security Assessor ("PSA") certification.   Submit an Attestation of Compliance ("AOC") Form   Mandatory Since Sep 2010   Every quarter:   Conduct a quarterly network scan by an Approved Scan Vendor ("ASV")	PCI Compliance   Status (Mondatory / Optional)   PCI Compliance   Status (Mondatory / Optional)

MasterCard's Compliance validation Requirements for Merchants Copyright © 2023 Global Risk Management Services Group L.L.C. All Rights Reserved.

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	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	<ol> <li>Qualified Security Assessor - QSA (Annual On-site Assessment)/Qualified Internal Resources (e.g ISA).</li> <li>Approved Scanning Vendor (ASV) for scanning reports</li> </ol>	<ol> <li>ROC template will be provided by your QSA/Qualified Internal resource</li> <li>ASV provides scanning reports</li> <li>Attestation of Compliance Form</li> </ol>		
<b>1 - 6 Million</b> <b>or</b> Any Level 2 criteria of Visa	2	➤ Every year: □ Complete a Self-Assessment Questionnaire ("SAQ"). □ Submit an Attestation of Compliance ("AOC") Form.	Mandatory	<ol> <li>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).</li> <li>Approved Scanning Vendor (ASV) for scanning reports</li> </ol>	<ol> <li>SAQ (Look at the <u>SAQ</u> requirements to select right SAQ form to be completed)</li> <li>ASV provides scanning reports</li> <li>Attestation of Compliance Form</li> </ol>		
20,000 to 1 Million MasterCard and Maestro e-Commerce but less than 1 Million total or Any Level 3 criteria of Visa	3	*Note: Compliance date is set by your acquiring bank for level 4  Merchants.	Mandatory	<ol> <li>Qualified Internal Assessor/Qualified Internal Resources (e.g ISA).</li> <li>Approved Scanning Vendor (ASV) for scanning reports</li> </ol>	<ol> <li>SAQ (Look at the <u>SAQ</u> <u>requirements</u> to select right SAQ         form to be completed)</li> <li>ASV provides scanning reports</li> <li>Attestation of Compliance Form</li> </ol>		
All others who not fall under above category or Any Level 4 criteria of Visa	4		Mandatory	<ol> <li>Qualified Internal Assessor/Qualified Internal Resources (e.g ISA).</li> <li>Approved Scanning Vendor (ASV) for scanning reports</li> </ol>	<ol> <li>SAQ (Look at the SAQ requirements to select right SAQ form to be completed)</li> <li>ASV provides scanning reports</li> <li>Attestation of Compliance Form</li> </ol>		
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							

Total # of

**Transactions** 

Annually

Levels

Requirements (What you have to do)

**Every year:**File a Report on Compliance ("ROC") by Qualified Security

	Master	Card's Compliance validation Requirements f	ior Service Provide	Copyright © 2023 Global Risk Ma	anagement Services Group L.L.C. All Rights Reserved.
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/proce ss 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	<ol> <li>Qualified Security         Assessor - QSA         (Annual On-site         Assessment).</li> <li>Approved Scanning         Vendor(ASV)</li> </ol>	<ol> <li>Annual on-site PCI data security assessment (ROC) by qualified security assessor (QSA).</li> <li>ASV provides scanning reports</li> </ol>
Any Data Storing Entities (DSE) that stores/transmit/proce ss 300,000 or less transaction (total combined Mastercard and Maestro transactions annually)	2	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  Fevery quarter:  Conduct a quarterly network scan by an Approved Scan Vendor ("ASV")	Mandatory Since Sep 2010	<ol> <li>QSA/Qualified         <ul> <li>Internal Resources</li> <li>(e.g ISA).</li> </ul> </li> <li>Approved Scanning         <ul> <li>Vendor(ASV)</li> </ul> </li> </ol>	<ol> <li>Annual on-site PCI data security assessment (SAQ-D) by QSA/ISA.</li> <li>ASV provides scanning reports</li> </ol>
Note: Merchant level identific	cation is based on the	e corporate entity's total volume of VISA transactions (inclusive of credit, debit and prepaid) meeting to locations (e.g., franchisee, licensee) may be excluded if it is		or with one acquirer per year. Volume fro	pm independently-owned and operated merchant

AMI	EX's Cor	mpliance validation Require	ements for Mer	chants / Service Providers	Copyright © 2023 Global Risk Management Services Group L.L.C. All Rights Reserved.
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	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	<ol> <li>Qualified Security Assessor - QSA         (Annual On-site         Assessment)/Qualified Internal         Resources (e.g ISA).</li> <li>Approved Scanning Vendor (ASV) for         scanning reports</li> <li>External Network Vulnerability Scan</li> </ol>	<ol> <li>Report on Compliance (ROC)</li> <li>Attestation of Compliance (AOC).</li> <li>Other acceptable documentation: American Express STEP Attestation</li> </ol>
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	<ol> <li>Qualified Internal Resources (e.g ISA) for Annual Self assessment.</li> <li>Approved Scanning Vendor (ASV) for scanning reports.</li> <li>External Network Vulnerability Scan</li> </ol>	<ol> <li>SAQ (Look at the <u>SAQ requirements</u> to select right SAQ form to be completed)</li> <li>ASV Scan Report Attestation of Scan Compliance (AOSC)</li> <li>Other acceptable documentation: Report on Compliance Attestation of Compliance (ROC AOC) American Express STEP Attestation</li> </ol>
Between 10,000 and 50,000	3		If required by American Express, otherwise optional	<ol> <li>Qualified Internal Resources (e.g ISA) for Annual Self assessment.</li> <li>Approved Scanning Vendor (ASV) for scanning reports.</li> <li>External Network Vulnerability Scan</li> </ol>	<ol> <li>SAQ (Look at the <u>SAQ requirements</u> to select right SAQ form to be completed)</li> <li>ASV Scan Report Attestation of Scan Compliance (AOSC)</li> <li>Other acceptable documentation: Report on Compliance Attestation of Compliance (ROC AOC) American Express STEP Attestation</li> </ol>
Less than 10,000	4		If required by American Express, otherwise optional	<ol> <li>Qualified Internal Resources (e.g ISA) for Annual Self assessment.</li> <li>Approved Scanning Vendor (ASV) for scanning reports.</li> </ol>	<ol> <li>SAQ (Look at the <u>SAQ requirements</u> to select right SAQ form to be completed)</li> <li>ASV Scan Report Attestation of Scan Compliance (AOSC)</li> <li>Other acceptable documentation: Report on Compliance Attestation of Compliance (ROC AOC) American Express STEP Attestation</li> </ol>
	Note: Mercha	ant level identification is based on the cornorate entity's tota	I volume of AMEX transactions (inc	lusive of credit. debit and prepaid) meeting the transaction t	hresholds in one country or with one acquirer per year

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	<ol> <li>Qualified Security Assessor -         QSA Qualified Internal         Resources (e.g ISA) For Annual             On-site Assessment         <ol> <li>Approved Scanning Vendor             (ASV) for scanning reports</li> </ol> </li> <li>External Network Vulnerability         <ol> <li>Scan</li> </ol> </li> </ol>	<ol> <li>Attestation of Compliance (AOC) from Report on Compliance (ROC)</li> <li>Submission of scan results not required</li> <li>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.</li> </ol>
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.	Mandatory for Merchants	<ol> <li>Qualified Internal Resources (e.g ISA) for Annual Self assessment.</li> <li>Approved Scanning Vendor (ASV) for scanning reports.</li> <li>External Network Vulnerability Scan</li> </ol>	Attestation of Compliance (AOC) from SAQ. For SAQ (Look at the SAQ requirements to select right SAQ form to be completed)     Submission of scan results not required
All other merchants	3	➤ 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	<ol> <li>Qualified Internal Resources (e.g ISA) for Annual Self assessment.</li> <li>Approved Scanning Vendor (ASV) for scanning reports.</li> <li>External Network Vulnerability Scan</li> </ol>	<ol> <li>Attestation of Compliance (AOC) from SAQ. For SAQ (Look at the SAQ requirements to select right SAQ form to be completed)</li> <li>Submission of scan results not required</li> </ol>

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	<ol> <li>Qualified Security Assessor - QSA         Qualified Internal Resources (e.g         ISA) For Annual On-site         Assessment</li> <li>Approved Scanning Vendor (ASV)         for scanning reports</li> </ol>	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	<ol> <li>Qualified Internal Resources (e.g ISA) for Annual Self assessment.</li> <li>Approved Scanning Vendor (ASV) for scanning reports.</li> </ol>	<ol> <li>Attestation of Compliance (AOC) from SAQ</li> <li>Submission of scan results not required</li> <li>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.</li> </ol>

JCB's Compliance v	<u>ralidatio</u>	n Requirements for Me	rchants / Servic	e Providers Copyright © 2023 Global Risk Manageme	ent Services Group L.L.C. All Rights Reserved.
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)	<ol> <li>Qualified Security Assessor - QSA Qualified Internal Resources (e.g ISA) For Annual On-site Assessment</li> <li>Approved Scanning Vendor (ASV) for scanning reports</li> <li>External Network Vulnerability Scan</li> <li>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.</li> </ol>	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)	<ol> <li>Qualified Internal Resources (e.g ISA) for Annual Self assessment.</li> <li>Approved Scanning Vendor (ASV) for scanning reports.</li> <li>External Network Vulnerability Scan</li> <li>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.</li> </ol>	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

## Self Assessment Questionnaire (SAQ) Requirements for Merchants/Service providers

right © 2023 Global Risk Management Services Group L.L.C. All Rights Reserved.

C https://docs-prv.pcisecuritystandards.org/SAQ (Assessment)/Instructions %26 Guidance/SAQ-InstrGuidelines-v3-2-1-r1.pdf \$ 21 of 21 110% Which SAQ Best Applies to My Environment? SAQ SELECTION INSTRUCTIONS Service Are you a Provider service provider? ✓ 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. Storage of Does merchant store Electronic any cardholder data, Merchants with more than one channel should consult with Cardholder Data including legacy data? their acquirer about how to validate compliance. Merchants must meet all eligibility criteria for any applicable SAQ. Does merchant **PCI-listed** SAQ accept transactions P2PE protected by a PCI-listed Solution P2PE Solution? Via merchant's Via payment Does merchant Via PTS Via imprint web browser app on POS accept card-present YES AND. AND. AND, sending to service Card-present or dial-out approved or PC transactions not machines. devices with provider's Transactions OR with Internet protected by a PCI-listed no Internet Internet "virtual payment connection P2PE solution? application" SAQ B-IP SAQ SAQ SAQ В C-VT Via merchant's Via CHD functions fully Does merchant Via payment Via PTS outsourced to a PCI DSS Via imprint web browser accept MOTO app on POS YES. мото AND, AND AND or dial-out approved AND. sending to service compliant service provider, no transactions not or PC devices with electronic CHD storage, OR machines, OR OR provider's **Transactions** OR with Internet protected by a PCI-listed no Internet Internet "virtual payment processing or transmission on P2PE solution? connection application" merchant systems or premises Via CHD functions fully outsourced to a Via payment processing outsourced to PCI DSS compliant service provider, including PCI DSS validated service provider, merchant Via systems Does merchant YES all elements of the payment page (for example, AND AND E-commerce website delivers some elements of the managed accept e-commerce via URL redirect or iFrame). No electronic CHD payment page (for example, via Direct Post). **Transactions** by the transactions? storage, processing or transmission on merchant No electronic CHD storage, processing or merchant systems or premises. transmission on merchant systems or premises. 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