PCI DSS Validation Best Practice Review

September 20, 2018

Ben Choong – Director, Ecosystem Data Security

VISA

Disclaimer

Notice

The information, recommendations or “best practices” contained herein are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations, programs or “best practices” may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions and expected future developments and other factors that we believe are appropriate under the circumstance.

Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error free. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

Agenda

1. Threat Landscape and Visa's Security Strategy
2. Understanding PCI DSS Compliance and Validation
3. Common Validation Documentation Errors
4. Using the Prioritized Approach
5. Data Security Resources
6. Q&A

Threat Landscape

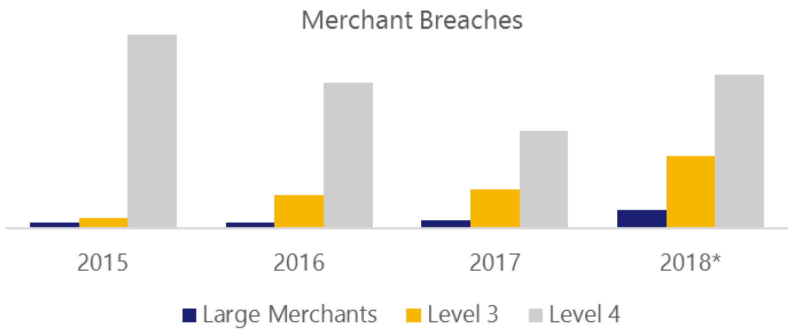
Global Compromise Trends

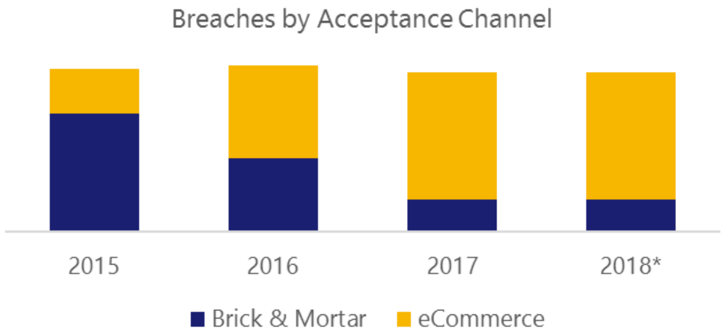
Shifting Breach Types

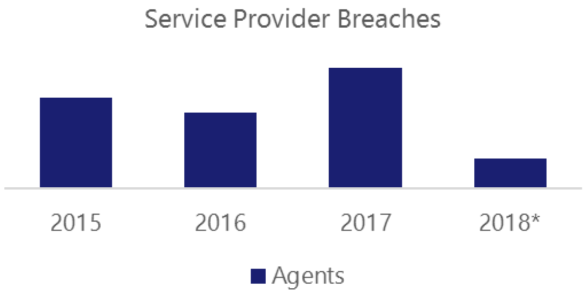
- Decrease in events involving magnetic stripe data
- Increase in eCommerce compromises
- Proliferation of third-party breaches

Criminals Moving Beyond Merchants

- Targeting data aggregators and integrators/resellers
- Increasing focus on eCommerce service providers
- Penetrating financial institutions


Merchant Breaches


Breaches by Acceptance Channel


Service Provider Breaches

Visa’s Security Strategy

Data is Key to Addressing Threats

Protect Data

Safeguard payment data

Harness Data

Stop fraud before it occurs

Devalue Data

Render data useless

Empower Consumers

Engage cardholders in payment security

Visa’s Account Information Security Program

Protection of Account Information is Critical

What is the Visa AIS Program?

- Global compliance program focused on the safeguarding of Visa account information across the payments ecosystem
- Establishes requirements for compliance and validation against industry security standards for Visa clients, merchants, processors, third party agents and other industry stakeholders

What are the Program Objectives?

- Maintain the safety and integrity of the Visa payments ecosystem
- Proactively defend against compromises of Visa account data through monitoring compliance and addressing security deficiencies
- Incentivize adoption of secure acceptance technologies and practices

PCI DSS: Understanding Compliance and Validation

Payment Card Industry Data Security Standard

Compliance + Validation

Compliance

- Visa requires **ALL** organizations that store, transmit or process Visa account data to comply with PCI DSS
- PCI DSS applies to all payment channels, including card present, mail/telephone order, eCommerce, in-app, etc.

Validation

- Separate and distinct from the requirement to comply with PCI DSS is the validation of compliance
- Validation is the exercise of verifying and demonstrating compliance status against the PCI DSS requirements

Stakeholder Roles and Responsibilities

Visa

- Establish and enforce compliance programs to ensure stakeholders protect data in accordance with industry standards
- Provide data security education and awareness on threats and mitigation strategies
- Promote use of secure acceptance technologies

Clients

- Ensure sponsored merchants and agents handling account data on their behalf comply with PCI DSS
- Provide status updates to Visa in accordance with the AIS Program

Merchants and Service Providers

- Protect Visa account data in accordance with PCI DSS and other applicable data security standards
- Validate compliance as required by Visa's AIS Program

PCI SSC

- Develop and manage the PCI DSS, validation tools, guidance documentation and supporting educational material
- Train and manage Qualified Security Assessors, Approved Scan Vendors, Qualified Integrators and Resellers, and other certification programs

PCI DSS Validation Requirements

Merchants

Level	Annual Transaction Volume	Minimum Validation Requirements
1	6 million+ Visa transactions (all channels)	• Report on Compliance (ROC) by Qualified Security Assessor (QSA) or internal resources if signed by officer of the company • Attestation of Compliance (AOC)
2	1 million to 6 million Visa transactions (all channels)	• Self-Assessment Questionnaire (SAQ) • Attestation of Compliance (AOC)
3	20,000 to 999,999 Visa eCommerce transactions	• Self-Assessment Questionnaire (SAQ) • Attestation of Compliance (AOC)
4	Less than 20,000 Visa eCommerce transactions and all other merchants processing less than 1 million Visa transactions	• Self-Assessment Questionnaire (SAQ) or alternative validation as defined by acquirer

Service Providers

Level	Annual Transaction Volume	Minimum Validation Requirements
1	More than 300,000 Visa transactions	• Report on Compliance (ROC) by Qualified Security Assessor (QSA) • Attestation of Compliance (AOC)
2	Less than 300,000 Visa transactions	• Self-Assessment Questionnaire (SAQ)* • Attestation of Compliance (AOC)

*Service providers must complete a full ROC using a PCI QSA in order to be included on Visa's Global Registry of Service Providers., regardless of level.

PCI DSS Validation Documentation

Report on Compliance (ROC)

- Report documenting detailed results from an entity's PCI DSS assessment against each individual requirement
- Template includes a thorough environmental summary (Sections 1 – 5), fields for individual PCI DSS requirement descriptions, testing procedures, reporting instructions and assessor responses.
- Report also includes supplemental appendices that may be applicable for certain entities

Self-Assessment Questionnaire (SAQ)

- Reporting tool used to document self-assessment results from an entity's PCI DSS assessment
- Questionnaire with a series of "YES or NO" questions for each applicable PCI DSS requirement
- There are 9 different questionnaires available to meet different acceptance environments

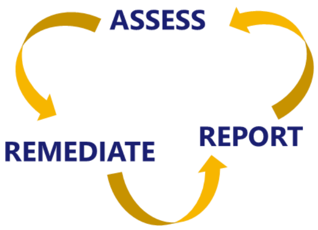
Attestation of Compliance (AOC)

- Form for merchants and service providers to attest to the results of a PCI DSS assessment, as documented in the ROC or SAQ

PCI DSS Validation Process

Compliance Assessment and Validation Steps:

PCI DSS COMPLIANCE IS A CONTINUOUS PROCESS



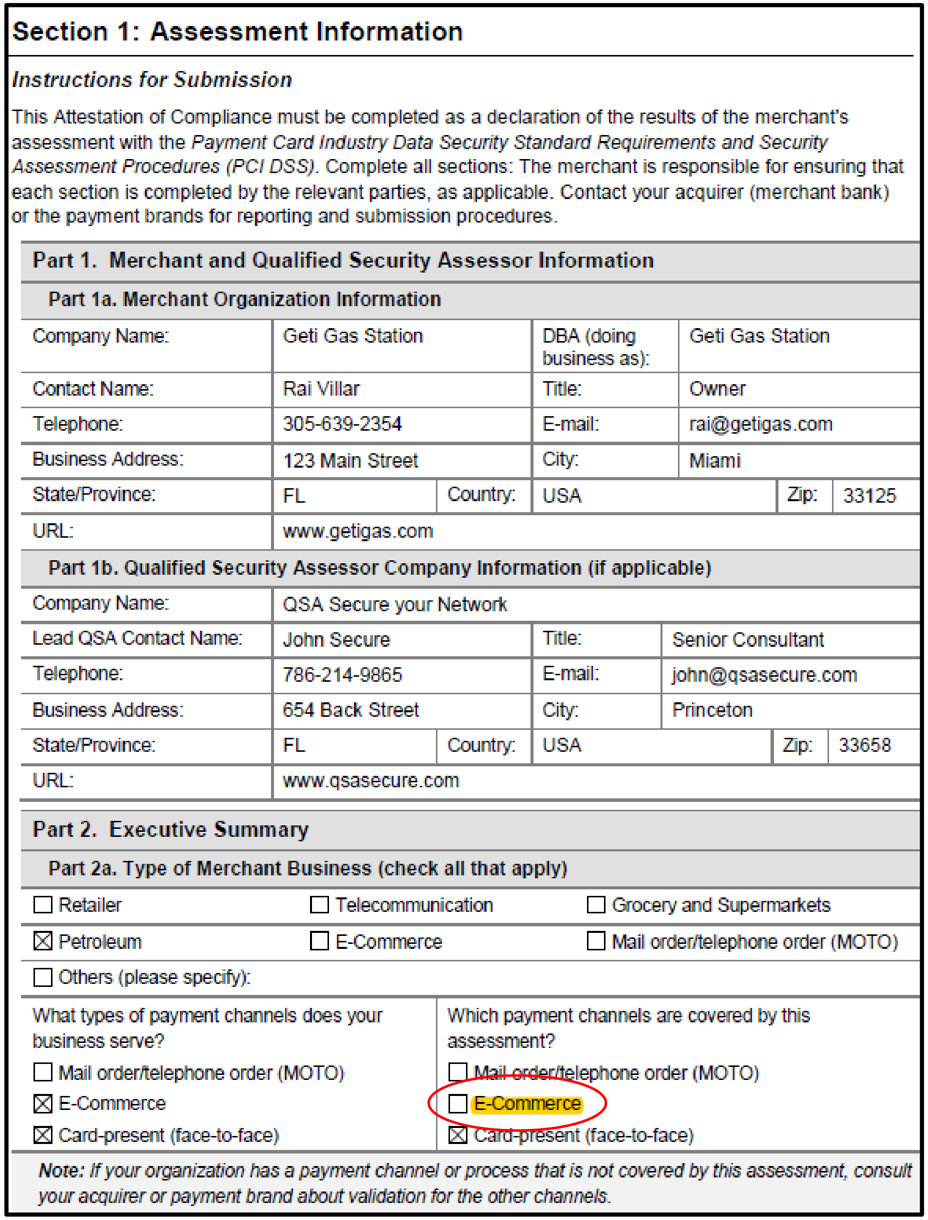
1. Scope – Determine which system components and networks are in scope for PCI DSS
2. Assess – Examine the compliance of system components in scope following the testing procedure for each PCI DSS requirement
3. Remediate – If required, perform remediation to address requirements that are not in place, and provide an updated report
4. Report – Assessor and/or entity completes required validation documentation (e.g. SAQ or ROC), including documentation of all compensating controls
5. Attest – Complete the appropriate Attestation of Compliance (AOC)
6. Submit – Submit the SAQ, ROC, AOC and other supporting documentation to the acquirer or Visa as required

Source: https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf?agreement=true&time=1536263962218

Common Validation Documentation Errors

Attestation of Compliance

Are all payment acceptance channels identified and assessed?



Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the merchant's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS).* Complete all sections: The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact your acquirer (merchant bank) or the payment brands for reporting and submission procedures.

Part 1. Merchant and Qualified Security Assessor Information

Part 1a. Merchant Organization Information

Company Name:	Geti Gas Station		DBA (doing business as):	Geti Gas Station	
Contact Name:	Rai Villar		Title:	Owner	
Telephone:	305-639-2354		E-mail:	rai@getigas.com	
Business Address:	123 Main Street		City:	Miami	
State/Province:	FL	Country:	USA	Zip:	33125
URL:	www.getigas.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:	QSA Secure your Network				
Lead QSA Contact Name:	John Secure		Title:	Senior Consultant	
Telephone:	786-214-9865		E-mail:	john@qsasecure.com	
Business Address:	654 Back Street		City:	Princeton	
State/Province:	FL	Country:	USA	Zip:	33658
URL:	www.qsasecure.com				

Part 2. Executive Summary

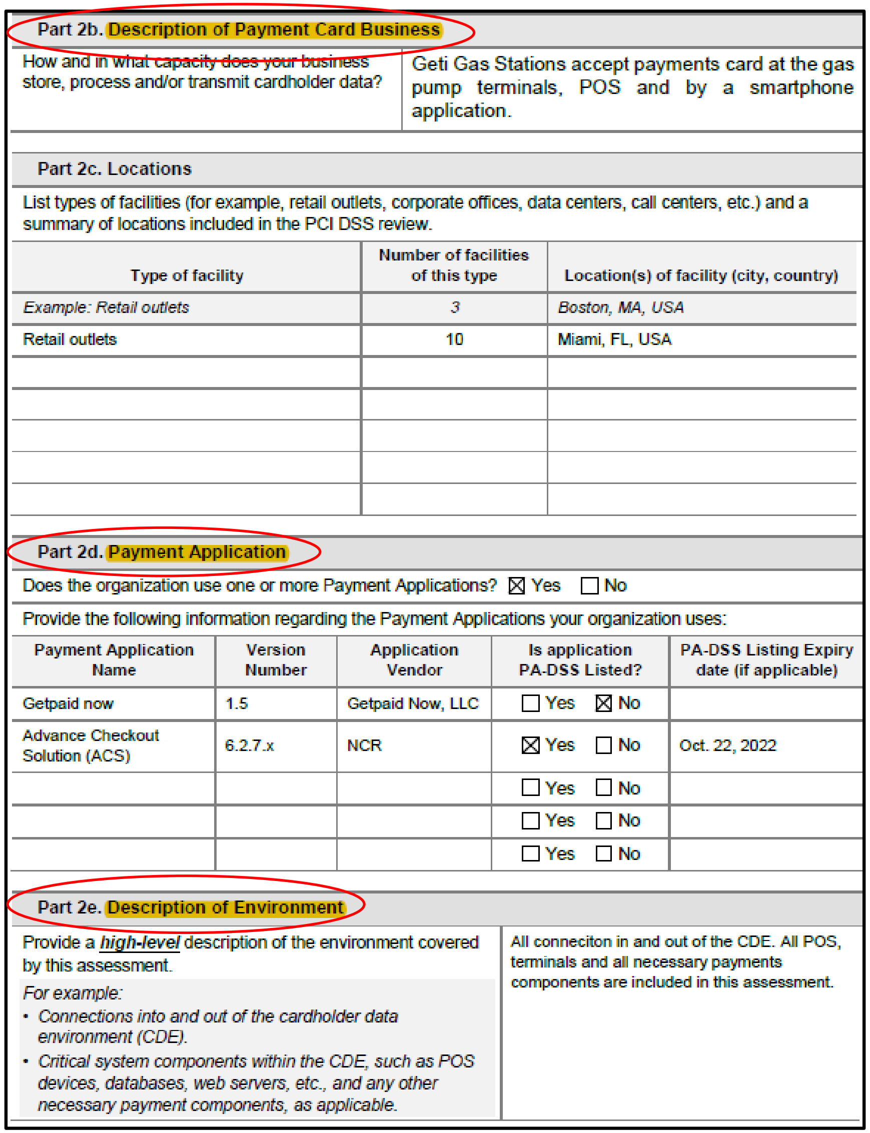
Part 2a. Type of Merchant Business (check all that apply)

□ Retailer	□ Telecommunication	□ Grocery and Supermarkets
☒ Petroleum	□ E-Commerce	□ Mail order/telephone order (MOTO)
□ Others (please specify):		

What types of payment channels does your business serve?	Which payment channels are covered by this assessment?
□ Mail order/telephone order (MOTO)	□ Mail order/telephone order (MOTO)
☒ E-Commerce	□ E-Commerce
☒ Card-present (face-to-face)	☒ Card-present (face-to-face)

Note: *If your organization has a payment channel or process that is not covered by this assessment, consult your acquirer or payment brand about validation for the other channels.*

Commonly Forgotten Descriptions . . .



Part 2b. Description of Payment Card Business

How and in what capacity does your business store, process and/or transmit cardholder data?	Geti Gas Stations accept payments card at the gas pump terminals, POS and by a smartphone application.

Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility	Number of facilities of this type	Location(s) of facility (city, country)
Example: Retail outlets	*3*	*Boston, MA, USA*
Retail outlets	10	Miami, FL, USA

Part 2d. Payment Application

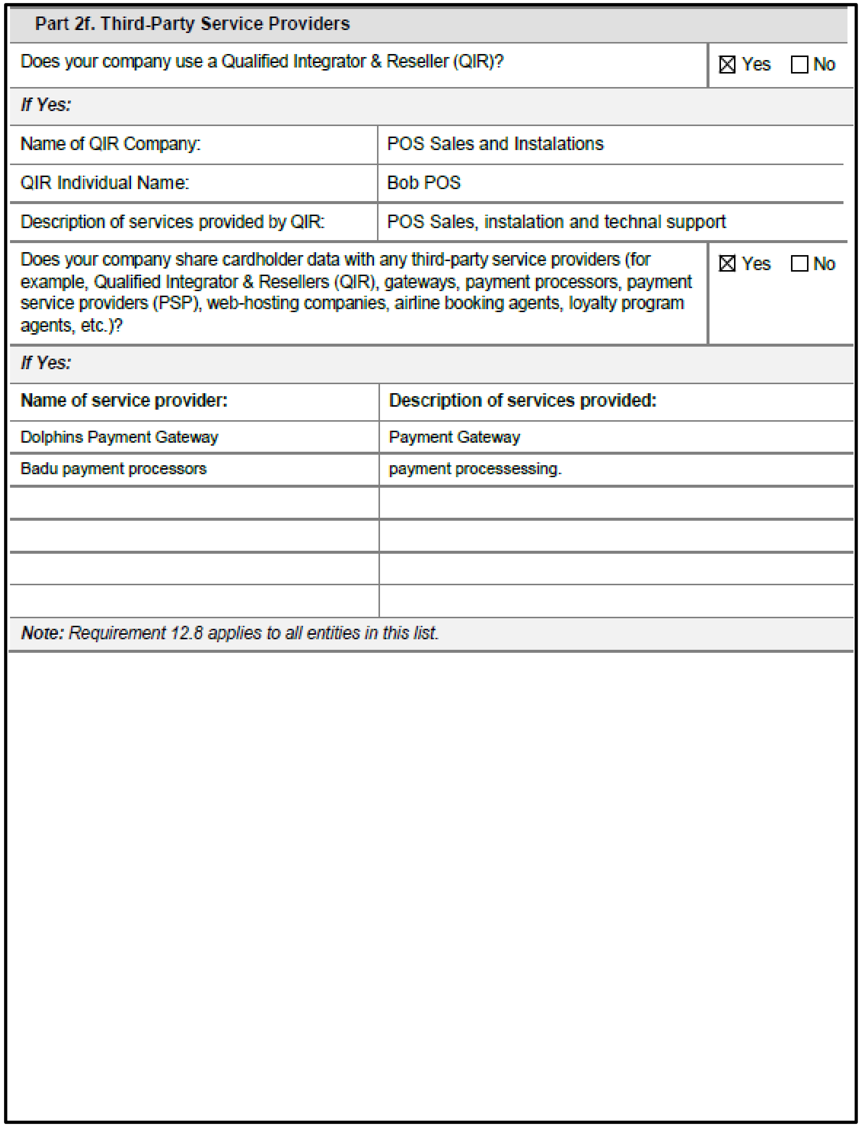
Does the organization use one or more Payment Applications? ☒ Yes ☐ No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
Getpaid now	1.5	Getpaid Now, LLC	☐ Yes ☒ No	
Advance Checkout Solution (ACS)	6.2.7.x	NCR	☒ Yes ☐ No	Oct. 22, 2022
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	

Part 2e. Description of Environment

Provide a ***high-level*** description of the environment covered by this assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	All conneciton in and out of the CDE. All POS, terminals and all necessary payments components are included in this assessment.



Part 2f. Third-Party Service Providers

Does your company use a Qualified Integrator & Reseller (QIR)?	☒ Yes ☐ No

If Yes:

Name of QIR Company:	POS Sales and Instalations
QIR Individual Name:	Bob POS
Description of services provided by QIR:	POS Sales, instalation and technal support

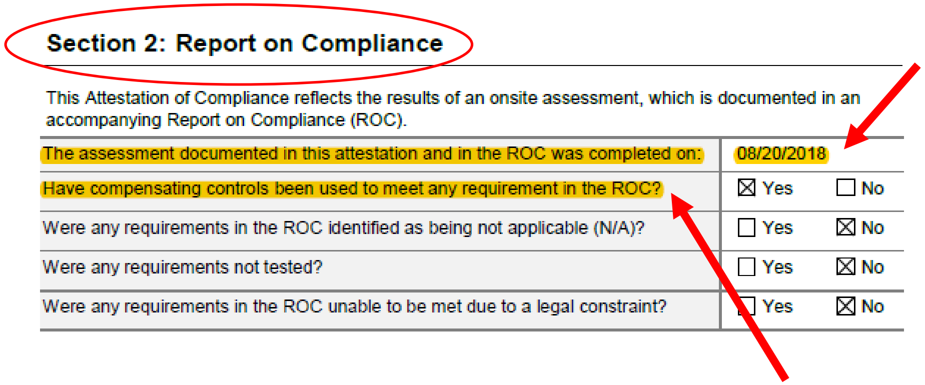
Does your company share cardholder data with any third-party service providers (for example, Qualified Integrator & Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.)?	☒ Yes ☐ No

If Yes:

Name of service provider:	Description of services provided:
Dolphins Payment Gateway	Payment Gateway
Badu payment processors	payment processessing.

***Note:** Requirement 12.8 applies to all entities in this list.*

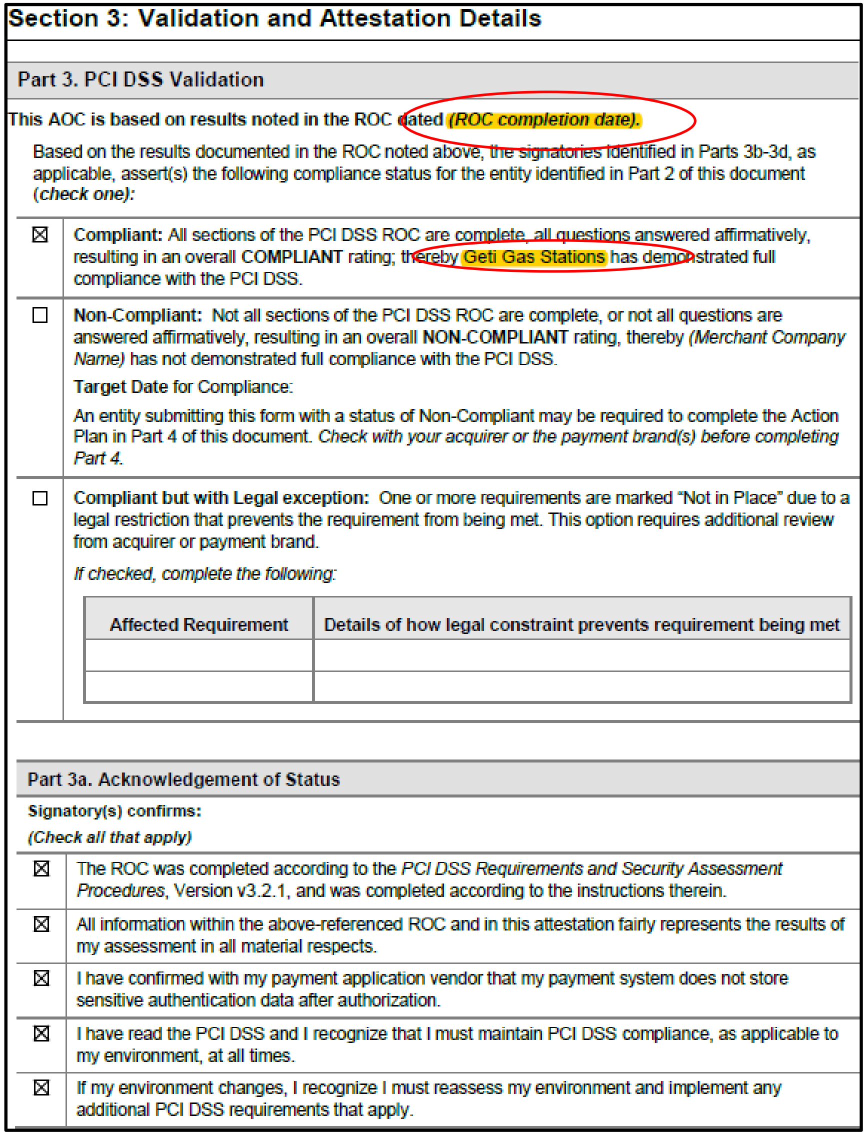
Check Those Boxes . . .



Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	08/20/2018
Have compensating controls been used to meet any requirement in the ROC?	☒ Yes ☐ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☐ Yes ☒ No
Were any requirements not tested?	☐ Yes ☒ No
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No



Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated *(ROC completion date).*

Based on the results documented in the ROC noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document ***(check one):***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby Geti Gas Stations has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *(Merchant Company Name)* has not demonstrated full compliance with the PCI DSS. Target Date for Compliance: An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with your acquirer or the payment brand(s) before completing Part 4.*
☐	**Compliant but with Legal exception:** One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met

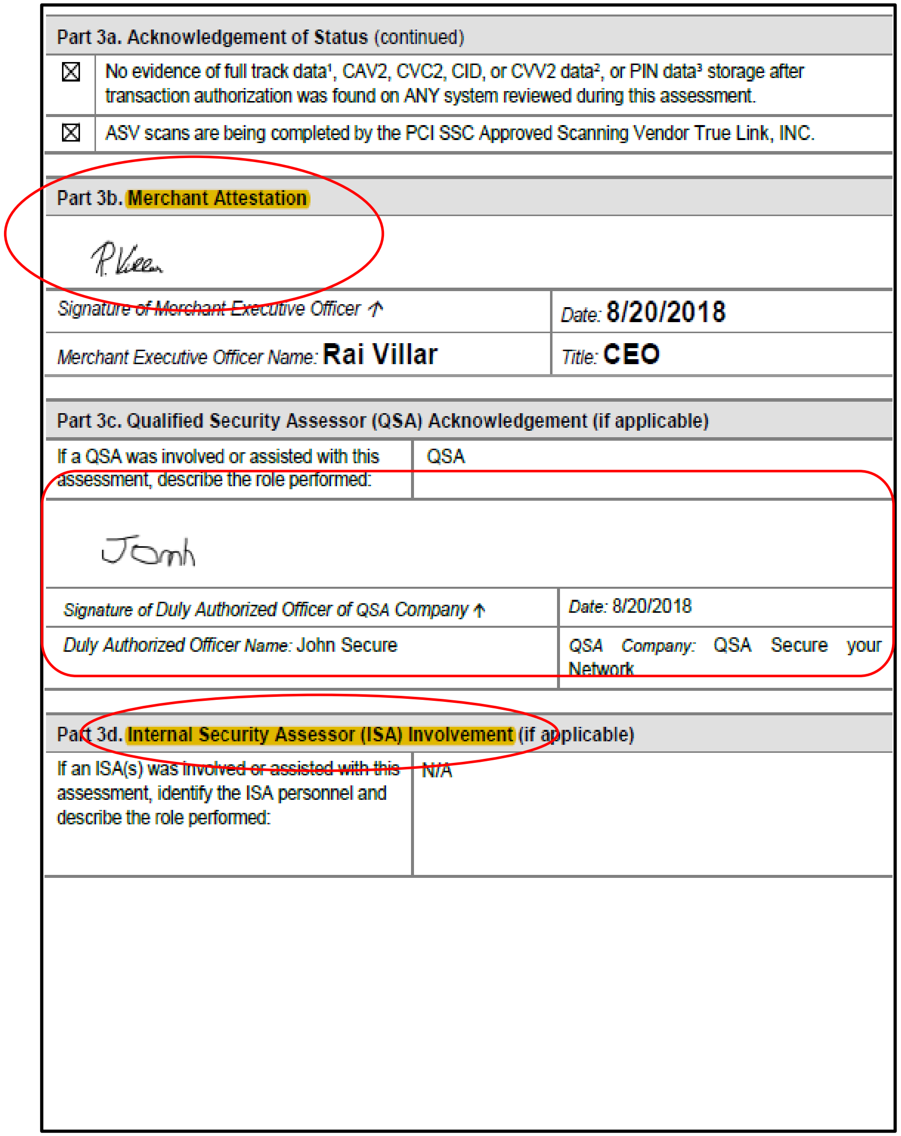
Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version v3.2.1, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
☒	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☒	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
☒	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

Signatures and Dates are Important!



Part 3a. Acknowledgement of Status (continued)

☒ No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.

☒ ASV scans are being completed by the PCI SSC Approved Scanning Vendor True Link, INC.

Part 3b. Merchant Attestation

P.Vee

Signature of Merchant Executive Officer ↑

Date: **8/20/2018**

Merchant Executive Officer Name: **Rai Villar**

Title: **CEO**

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	QSA

Jomh

Signature of Duly Authorized Officer of QSA Company ↑

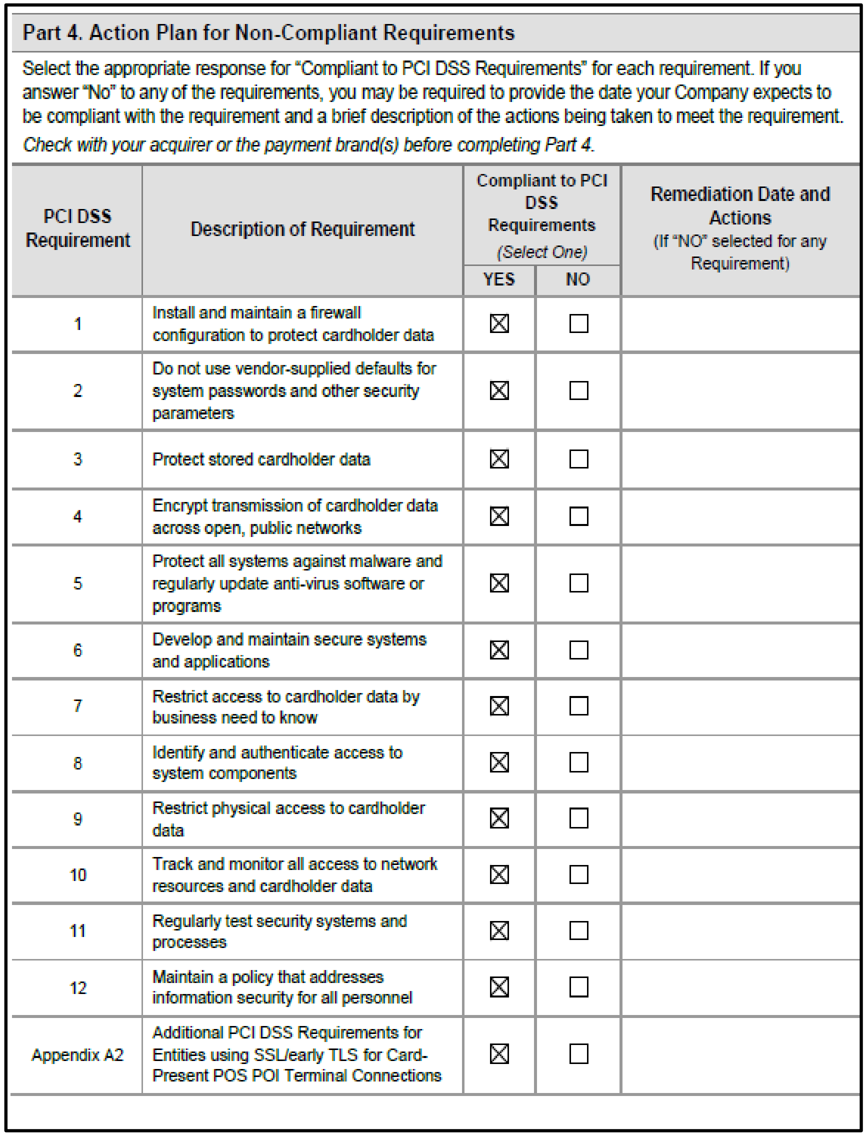
Date: 8/20/2018

Duly Authorized Officer Name: John Secure

QSA Company: QSA Secure your Network

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	N/A



Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement. *Check with your acquirer or the payment brand(s) before completing Part 4.*

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements *(Select One)*		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
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	☒	□	
3	Protect stored cardholder data	☒	□	
4	Encrypt transmission of cardholder data across open, public networks	☒	□	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	□	
6	Develop and maintain secure systems and applications	☒	□	
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	☒	□	
10	Track and monitor all access to network resources and cardholder data	☒	□	
11	Regularly test security systems and processes	☒	□	
12	Maintain a policy that addresses information security for all personnel	☒	□	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☒	□	

PCI DSS and the Prioritized Approach

Prioritizing the Approach to PCI DSS Compliance

Reducing Risk Earlier in the Compliance Process

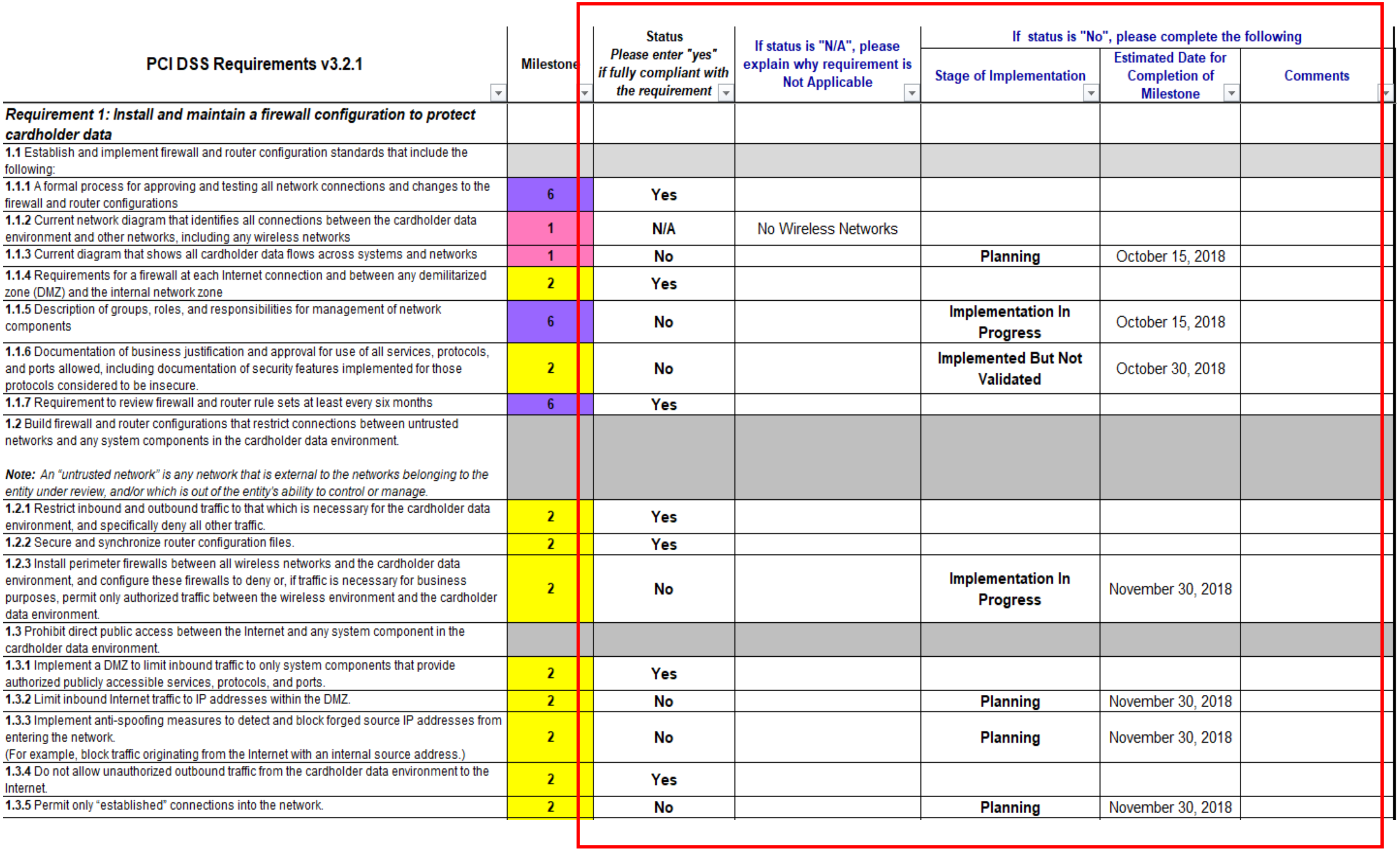
PCI SSC Prioritized Approach

- Provides six security milestones to help organizations incrementally protect against the highest risk factors while working towards PCI DSS compliance
- Serves as a roadmap for prioritizing implementation of security controls
- Supports financial and operational planning
- Promotes objective and measurable progress indicators

Reminders!

- The Prioritized Approach is not a substitute, short cut or stop gap approach to PCI DSS compliance
- It is not mandatory or suitable for all organizations to use or follow the Prioritized Approach
- To achieve PCI DSS compliance, organizations must meet all PCI DSS requirements, regardless of the order in which they are implemented

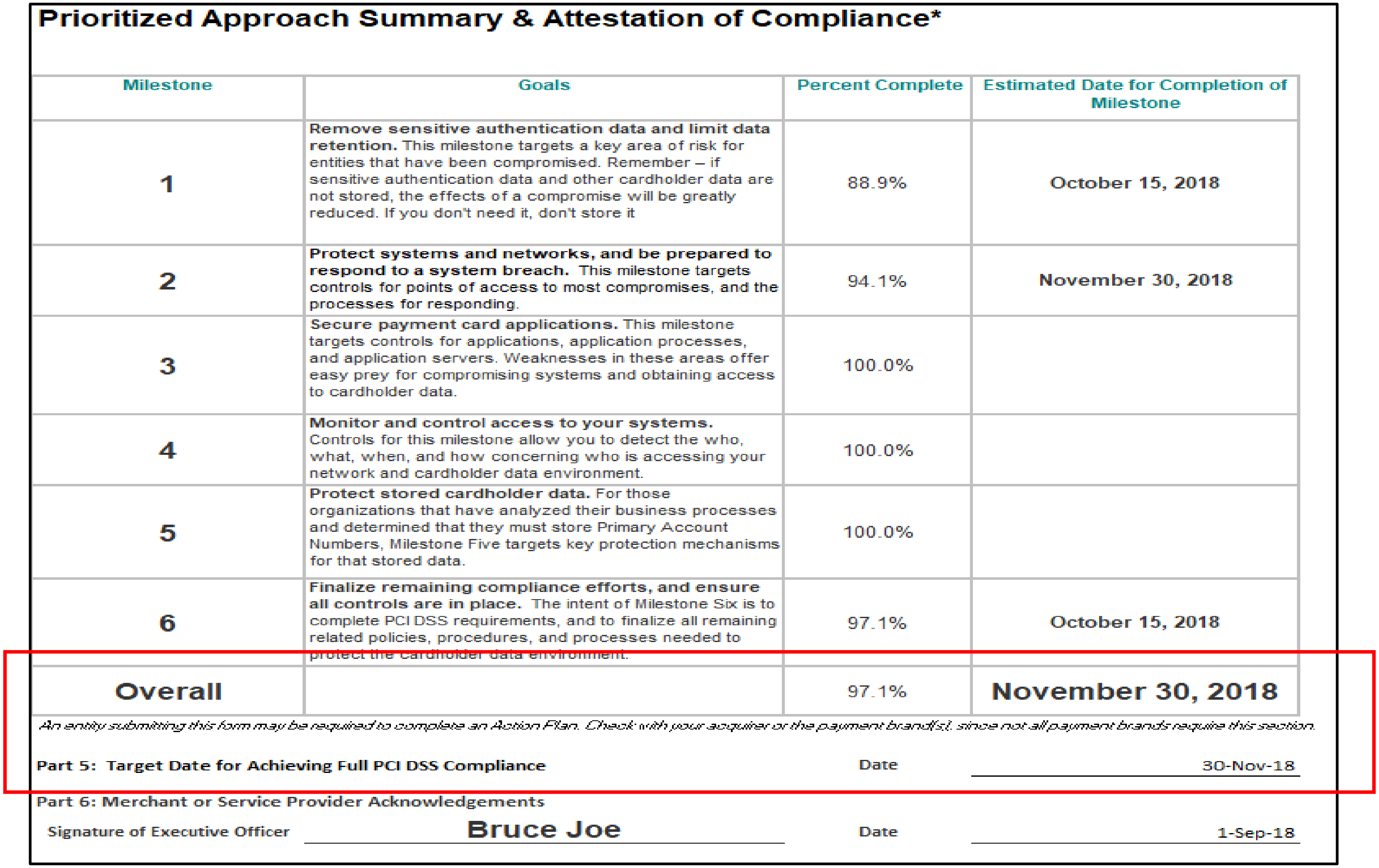
Ensure the Plan is Complete



PCI DSS Requirements v3.2.1	Milestone	Status *Please enter "yes" if fully compliant with the requirement*	If status is "N/A", please explain why requirement is Not Applicable	If status is "No", please complete the following		
				Stage of Implementation	Estimated Date for Completion of Milestone	Comments
Requirement 1: Install and maintain a firewall configuration to protect cardholder data						
1.1 Establish and implement firewall and router configuration standards that include the following:						
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	6	Yes				
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	1	N/A	No Wireless Networks			
1.1.3 Current diagram that shows all cardholder data flows across systems and networks	1	No		Planning	October 15, 2018	
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	2	Yes				
1.1.5 Description of groups, roles, and responsibilities for management of network components	6	No		Implementation In Progress	October 15, 2018	
1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	2	No		Implemented But Not Validated	October 30, 2018	
1.1.7 Requirement to review firewall and router rule sets at least every six months	6	Yes				
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. ***Note:*** *An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*						
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	2	Yes				
1.2.2 Secure and synchronize router configuration files.	2	Yes				
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	2	No		Implementation In Progress	November 30, 2018	
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.						
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	2	Yes				
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	2	No		Planning	November 30, 2018	
1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)	2	No		Planning	November 30, 2018	
1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	2	Yes				
1.3.5 Permit only "established" connections into the network.	2	No		Planning	November 30, 2018	

Milestone Completion Dates

Review and Recognize Reasonable Completion Targets



Prioritized Approach Summary & Attestation of Compliance*

Milestone	Goals	Percent Complete	Estimated Date for Completion of Milestone
1	**Remove sensitive authentication data and limit data retention.** This milestone targets a key area of risk for entities that have been compromised. Remember – if sensitive authentication data and other cardholder data are not stored, the effects of a compromise will be greatly reduced. If you don't need it, don't store it	88.9%	October 15, 2018
2	**Protect systems and networks, and be prepared to respond to a system breach.** This milestone targets controls for points of access to most compromises, and the processes for responding.	94.1%	November 30, 2018
3	**Secure payment card applications.** This milestone targets controls for applications, application processes, and application servers. Weaknesses in these areas offer easy prey for compromising systems and obtaining access to cardholder data.	100.0%	
4	**Monitor and control access to your systems.** Controls for this milestone allow you to detect the who, what, when, and how concerning who is accessing your network and cardholder data environment.	100.0%	
5	**Protect stored cardholder data.** For those organizations that have analyzed their business processes and determined that they must store Primary Account Numbers, Milestone Five targets key protection mechanisms for that stored data.	100.0%	
6	**Finalize remaining compliance efforts, and ensure all controls are in place.** The intent of Milestone Six is to complete PCI DSS requirements, and to finalize all remaining related policies, procedures, and processes needed to protect the cardholder data environment.	97.1%	October 15, 2018
Overall		97.1%	**November 30, 2018**

An entity submitting this form may be required to complete an Action Plan. Check with your acquirer or the payment brand(s), since not all payment brands require this section.

Part 5: Target Date for Achieving Full PCI DSS Compliance Date 30-Nov-18

Part 6: Merchant or Service Provider Acknowledgements

Signature of Executive Officer **Bruce Joe** Date 1-Sep-18

Consider Scope Reduction Opportunities

Less Data = Less Risk

Point-to-Point Encryption (P2PE)

- Implement PCI-validated P2PE solution to encrypt account data throughout lifecycle of transaction with no possible decryption in the merchant environment

Network Segmentation

- Establish a network framework which uses secure tools and processes to isolate the account data environment from the remainder of the network

Outsourcing

- Outsource payment acceptance and data processing to a PCI-validated service provider included on Visa’s Global Registry of Service Providers

EMVCo Tokenization

- Begin acceptance of payment tokens generated in accordance with the EMVCo Tokenization Specification to eliminate sensitive account data

Data Security Resources

Data Security Resources

Visa Data Security Website www.visa.com/cisp

- Alerts, Bulletins
- Best Practices, White Papers, Webinars

Visa Global Registry of Service Providers www.visa.com/onthelist

- List of registered, PCI DSS validated third party agents

PCI Security Standards Council Website www.pcissc.org

- Data Security Standards, Qualified Assessor Listings, Data Security Education Materials

PCI Resources for Small Merchants https://www.pcisecuritystandards.org/merchants/

- Guide to Safe Payments, Common Payment Systems, Questions to Ask your Vendors
- Payment Data Security Essentials: Video and Infographics

Visa’s Ecosystem Data Security Team

Questions? Comments?

- Agent Registration: agentregistration@visa.com
- Third Party Compliance: pcirocs@visa.com
- Merchant Compliance: cisp@visa.com
- ACS/AVP: AVPamericas@visa.com
- PIN security: pinna@visa.com

Q&A

Thank You