



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

---

## **Attestation of Compliance for Self-Assessment Questionnaire D – Merchants**

**For use with PCI DSS Version 3.2.1**

July 2018

## Section 1: Assessment Information

### Instructions for Submission

This document must be completed as a declaration of the results of the merchant's self-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 to determine reporting and submission procedures.

### Part 1. Merchant and Qualified Security Assessor Information

#### Part 1a. Merchant Organization Information

Company Name:	Schiphol Travel International	DBA (doing business as):	Schiphol Travel International		
Contact Name:	Michiel Prins	Title:	Project Manager		
Telephone:	+31 20 4055870	E-mail:	Michiel.Prins@Schipholtravel.com		
Business Address:	Schiphol Boulevard 235	City:	Luchthaven Schiphol		
State/Province:	Noord-Holland	Country:	The Netherlands	Zip:	1118 BH
URL:	www.schipholtravel.com				

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

Company Name:	Noordbeek B.V.				
Lead QSA Contact Name:	E. van Egmond	Title:	Senior Manager IT Audit		
Telephone:	06-233 26 272	E-mail:	edward.van.egmond@noordbeek.com		
Business Address:	Rijndijk 235	City:	Hazerswoude-Rijndijk		
State/Province:	Zuid-Holland	Country:	The Netherlands	Zip:	2394 CD
URL:	www.noordbeek.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): Travel Agent

What types of payment channels does your business serve?

- Mail order/telephone order (MOTO)  
 E-Commerce  
 Card-present (face-to-face)

Which payment channels are covered by this SAQ?

- Mail order/telephone order (MOTO)  
 E-Commerce  
 Card-present (face-to-face)

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

### Part 2b. Description of Payment Card Business

How and in what capacity does your business store, process and/or transmit cardholder data?

When the customer pays by credit card via telephone, the number is directly entered in a software solution. Another channel is via the website, when the customer enters his details the credit card is stored in the software. The payment handling is done via the software.

### 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)
<i>Example: Retail outlets</i>	3	<i>Boston, MA, USA</i>
Office	1	Luchthaven Schiphol

### 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)
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> 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.*

The office, to ensure no credit card data is written down or entered in other applications before entering in the software.

Does your business use network segmentation to affect the scope of your PCI DSS

Yes  No

environment?  
*(Refer to “Network Segmentation” section of PCI DSS for guidance on network segmentation)*

**Part 2f. Third-Party Service Providers**

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

**If Yes:**

Name of QIR Company:	
QIR Individual Name:	
Description of services provided by QIR:	

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:

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

## Section 2: Self-Assessment Questionnaire D – Merchants

This Attestation of Compliance reflects the results of a self-assessment, which is documented in an accompanying SAQ.

The assessment documented in this attestation and in the SAQ was completed on:	<i>20 February 2019</i>	
Have compensating controls been used to meet any requirement in the SAQ?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the SAQ identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Were any requirements in the SAQ identified as being not tested?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the SAQ unable to be met due to a legal constraint?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No

## Section 3: Validation and Attestation Details

### Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ D (Section 2), dated 20 February 2019.

Based on the results documented in the SAQ D 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)**:

<input checked="" type="checkbox"/>	<p><b>Compliant:</b> All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall <b>COMPLIANT</b> rating; thereby Schiphol Travel International has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p><b>Non-Compliant:</b> Not all sections of the PCI DSS SAQ are complete, or not all questions are answered affirmatively, resulting in an overall <b>NON-COMPLIANT</b> rating, thereby <i>(Merchant Company Name)</i> has not demonstrated full compliance with the PCI DSS.</p> <p><b>Target Date</b> for Compliance:</p> <p>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. <i>Check with your acquirer or the payment brand(s) before completing Part 4.</i></p>						
<input type="checkbox"/>	<p><b>Compliant but with Legal exception:</b> One or more requirements are marked “No” due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.</p> <p><i>If checked, complete the following:</i></p> <table border="1" style="width: 100%;"> <thead> <tr> <th style="width: 35%;">Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met				
Affected Requirement	Details of how legal constraint prevents requirement being met						

### Part 3a. Acknowledgement of Status

Signatory(s) confirms:

**(Check all that apply)**

<input checked="" type="checkbox"/>	PCI DSS Self-Assessment Questionnaire D, Version 3.2.1, was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
<input type="checkbox"/>	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

**Part 3a. Acknowledgement of Status (continued)**

<input checked="" type="checkbox"/>	No evidence of full track data <sup>1</sup> , CAV2, CVC2, CID, or CVV2 data <sup>2</sup> , or PIN data <sup>3</sup> storage after transaction authorization was found on ANY system reviewed during this assessment.
<input checked="" type="checkbox"/>	ASV scans are being completed by the PCI SSC Approved Scanning Vendor <i>Trustguard</i>

**Part 3b. Merchant Attestation**

Signature of Merchant Executive Officer ↑	Date: <b>20 February 2019</b>
Merchant Executive Officer Name: <i>D. Lenderink</i>	Title: <b>Director/Owner</b>

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

If a QSA was involved or assisted with this assessment, describe the role performed:	The QSA assessed the scope and reviewed the evidence.
--	---



Signature of Duly Authorized Officer of QSA Company ↑	Date: <b>20 February 2019</b>
Duly Authorized Officer Name: <b>E. van Egmond</b>	QSA Company: <b>Noordbeek B.V.</b>

**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:	
---	--

<sup>1</sup> Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

<sup>2</sup> The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

<sup>3</sup> Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

## 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	<input type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identify and authenticate access to system components	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	<input type="checkbox"/>	<input type="checkbox"/>	

