



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

Attestation of Compliance for Self-Assessment Questionnaire A

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:	Philip Morris International Management SA	DBA (doing business as):	IQOS		
Contact Name:	Jerome Redon	Title:	VP IS Business Engagement, RRP and Commercial		
Telephone:	+41 58 242 5652	E-mail:	jerome.redon@pmi.com		
Business Address:	Chemin de Brillancourt 4	City:	Lausanne		
State/Province:	Vaud	Country:	Switzerland	Zip:	1001
URL:	https://www.iqos.de , https://www.iqos.dk , https://www.iqos.nl , https://www.iqos.co.uk , https://www.iqos.co.il , https://www.iqos.kz , https://www.iqos.ca , https://www.iqos.co.nz				

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

Company Name:	Secureworks Limited				
Lead QSA Contact Name:	Kin-Ming Looi	Title:	Senior Principal Consultant		
Telephone:	+44 7753 297 662	E-mail:	klooi@secureworks.com		
Business Address:	One Creechurch Place 1 Creechurch Lane	City:	London		
State/Province:		Country:	United Kingdom	Zip:	EC3A 5AY
URL:	https://www.secureworks.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? <input type="checkbox"/> Mail order/telephone order (MOTO) <input checked="" type="checkbox"/> E-Commerce	Which payment channels are covered by this SAQ? <input type="checkbox"/> Mail order/telephone order (MOTO) <input checked="" type="checkbox"/> 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 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?

PMI has separate websites for those of its national markets supporting ecommerce. In some of those markets, PMI sells directly to consumers and so acts as a Merchant for PCI DSS compliance purposes (Germany, Denmark, Netherlands, United Kingdom, Israel, Kazakhstan, Canada and New Zealand) and this scope is the subject of this SAQ.

The websites for the following markets use a common design but are implemented separately: Germany, Denmark, Netherlands, United Kingdom, Israel, Kazakhstan, Canada and New Zealand.

Depending on the market, the customer is either:

- Redirected to an externally hosted payment processor page for the entry of payment card details (Kazakhstan and New Zealand) or;

- Presented with an externally-hosted payment processor page in an iframe for the entry of payment card details (all other markets).

PMI entities do not store CHD in any form.

In a number of other markets, PMI operates a website which is used by consumers but sales are made through a reseller partner. In those markets, PMI is acting as a Service Provider for its resellers; this will be the subject of a separate Service Provider SAQ and AOC.

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>
N/A	N/A	N/A

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)
PayNext payment gateway (Germany, Denmark, Netherlands, United Kingdom, Israel, Canada)	N/A	Arvato	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	N/A
Kazkom ePay payment gateway (Kazakhstan only)	N/A	Kazkom	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	N/A
Payment Express payment gateway (New Zealand only)	N/A	Payment Express	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	N/A
			<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.*

Connections:

General Internet connectivity to website and connectivity between website and payment gateway.

Systems:

Internet web servers:
DCS application controlling configuration of redirection or iframe to externally hosted payment gateway and page.

Processes:

Online Internet card payments.

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

(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)

Yes No

Part 2f. Third-Party Service Providers

Does your company use a Qualified Integrator & Reseller (QIR)?

Yes No

If Yes:	
Name of QIR Company:	N/A
QIR Individual Name:	N/A
Description of services provided by QIR:	N/A
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.)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

If Yes:	
Name of service provider:	Description of services provided:
Blue Infinity	Management of DCS website ecommerce platform.
Arvato	Hosted payment gateway providing iframe to payment processors. PayOn payment processor (all markets except Kazakhstan and New Zealand),
Kazkom (Kazakhstan only)	Payment processor
Payment Express (New Zealand only)	Payment processor

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

Part 2g. Eligibility to Complete SAQ A

Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because, for this payment channel:

- Merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions);
- All processing of cardholder data is entirely outsourced to PCI DSS validated third-party service providers;
- Merchant does not electronically store, process, or transmit any cardholder data on merchant systems or premises, but relies entirely on a third party(s) to handle all these functions;
- Merchant has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; **and**
- Any cardholder data the merchant retains is on paper (for example, printed reports or receipts), and these documents are not received electronically.
- Additionally, for e-commerce channels:*
All elements of the payment page(s) delivered to the consumer's browser originate only and directly from a PCI DSS validated third-party service provider(s).

Section 2: Self-Assessment Questionnaire A

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:	2
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 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 A (Section 2), dated 21-DEC-2018.

Based on the results documented in the SAQ A 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>Compliant: All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby <i>Philip Morris International Management SA</i> has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p>Non-Compliant: Not all sections of the PCI DSS SAQ are complete, or not all questions are answered affirmatively, resulting in an overall NON-COMPLIANT rating, thereby <i>(Merchant Company Name)</i> has not demonstrated full compliance with the PCI DSS.</p> <p>Target Date 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>Compliant but with Legal exception: 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 A, 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 checked="" 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)

- No evidence of full track data¹, CAV2, CVC2, CID, or CVV2 data², or PIN data³ 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 *Secureworks*

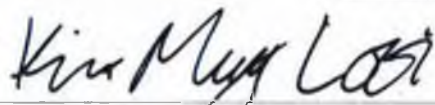
Part 3b. Merchant Attestation



Signature of Merchant Executive Officer ↑	Date: 8/2/2019
Merchant Executive Officer Name: Jerome Reaton	Title: VP Digital Platform Eng. Services

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

If a QSA was involved or assisted with this assessment, describe the role performed:	Conducted formal onsite assessment of scope, documentation (including network and CHD flow diagrams, standards, policies, procedures and evidence the procedures were followed), system settings and database contents (to confirm absence of stored CHD). Assessment resulted in production of SAQ and AOC by QSA.
--	---



Signature of Duly Authorized Officer of QSA Company ↑	Date: 31-JAN-2019
Duly Authorized Officer Name: Kin-Ming Looi	QSA Company: Secureworks Limited

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:	Not applicable
---	----------------

¹ 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.

² 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.

³ 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	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

* PCI DSS Requirements indicated here refer to the questions in Section 2 of the SAQ.

