



Payment Card Industry (PCI) Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2

April 2016

Section 1: Assessment Information

Instructions for Submission

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

Part 1. Service Provider and Qualified Security Assessor Information

Part 1a. Service Provider Organization Information

Company Name:	VINDI TECNOLOGIA E MARKETING S/A	DBA (doing business as):	VINDI
Contact Name:	Teogenes Panella	Title:	Information Security Manager
Telephone:	+55 11 5904-7380	E-mail:	teogenes.panella@vindi.com.br
Business Address:	Rua Sena Madureira, 163	City:	São Paulo
State/Province:	São Paulo	Country:	Brazil
		Zip:	04037-002
URL:	https://www.vindi.com.br		

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

Company Name:	CIPHER S/A		
Lead QSA Contact Name:	Paulo Rogerio de Aguiar Poi	Title:	Information Security Manager
Telephone:	+55 11 4501-6600 Ext.1446	E-mail:	ppoi@cipher.com
Business Address:	Rua Alexandre Dumas, 1658 - 2nd floor	City:	São Paulo
State/Province:	São Paulo	Country:	Brazil
		Zip:	04717-004
URL:	https://cipher.com/		

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) assessed: Payment Gateway

Type of service(s) assessed:

Hosting Provider:

- Applications / software
- Hardware
- Infrastructure / Network
- Physical space (co-location)
- Storage
- Web
- Security services
- 3-D Secure Hosting Provider
- Shared Hosting Provider
- Other Hosting (specify):

Managed Services (specify):

- Systems security services
- IT support
- Physical security
- Terminal Management System
- Other services (specify):

Payment Processing:

- POS / card present
- Internet / e-commerce
- MOTO / Call Center
- ATM
- Other processing (specify):

Account Management

Fraud and Chargeback

Payment Gateway/Switch

Back-Office Services

Issuer Processing

Prepaid Services

Billing Management

Loyalty Programs

Records Management

Clearing and Settlement

Merchant Services

Tax/Government Payments

Network Provider

Others (specify):

Note: These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.

Part 2a. Scope Verification *(continued)*

Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) not assessed: N/A

Type of service(s) not assessed:

Hosting Provider:	Managed Services (specify):	Payment Processing:
<input type="checkbox"/> Applications / software	<input type="checkbox"/> Systems security services	<input type="checkbox"/> POS / card present
<input type="checkbox"/> Hardware	<input type="checkbox"/> IT support	<input type="checkbox"/> Internet / e-commerce
<input type="checkbox"/> Infrastructure / Network	<input type="checkbox"/> Physical security	<input type="checkbox"/> MOTO / Call Center
<input type="checkbox"/> Physical space (co-location)	<input type="checkbox"/> Terminal Management System	<input type="checkbox"/> ATM
<input type="checkbox"/> Storage	<input type="checkbox"/> Other services (specify):	<input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Web		
<input type="checkbox"/> Security services		
<input type="checkbox"/> 3-D Secure Hosting Provider		
<input type="checkbox"/> Shared Hosting Provider		
<input type="checkbox"/> Other Hosting (specify):		
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Network Provider		
<input type="checkbox"/> Others (specify):		

Provide a brief explanation why any checked services were not included in the assessment: N/A

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	VINDI is a payment gateway that works with recurring transactions and their customers are companies that work with monthly subscriptions such as magazines, gyms and subscription clubs.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	VINDI process over 8 million transactions per year.

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	Boston, MA, USA
Corporate Office	1	São Paulo, SP, Brazil
Cloud Datacenter	N	Amazon Web Services, Worldwide

--	--	--

Part 2d. Payment Applications

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	
			<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.*

VINDI transmits and processes cardholder data from card-not-present transactions and forwards it to acquirers on behalf of merchants who contract their services. The company store cardholder data securely within its environment, and it is responsible for providing the network infrastructure to capture electronic transactions based secure services and responsible for "transmission" of transactions from payment API to the authorization systems.

The company receives cardholder data using their web portal and stores it securely within its environment, using strong encryption and managing keys with AWS KMS solution.

The company receives PAN, Card Validation Code, Expiry Date and Cardholder Name, however it does not store Card Validation Code after the authorization.

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

Yes No

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

Part 2f. Third-Party Service Providers

<p>Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated?</p> <p>If Yes:</p> <p style="padding-left: 20px;">Name of QIR Company:</p> <p style="padding-left: 20px;">QIR Individual Name:</p> <p style="padding-left: 20px;">Description of services provided by QIR:</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p>
<p>Does your company have a relationship with one or more 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.) for the purpose of the services being validated?</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p>

If Yes:

Name of service provider:	Description of services provided:
CIPHER	Support and guidance while assessing controls for PCI-DSS certification recommendation.
Amazon	PCI Compliant Cloud Service Provider

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

Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as “Not Tested” or “Not Applicable” in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as “Not Tested” or “Not Applicable” in the ROC.
- **None** – All sub-requirements of that requirement were marked as “Not Tested” and/or “Not Applicable” in the ROC.

For all requirements identified as either “Partial” or “None,” provide details in the “Justification for Approach” column, including:

- Details of specific sub-requirements that were marked as either “Not Tested” and/or “Not Applicable” in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

Note: One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.

Name of Service Assessed:		Payment Gateway		
	Details of Requirements Assessed			
PCI DSS Requirement	Full	Partial	None	Justification for Approach <small>(Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)</small>
Requirement 1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1.2.2 - The configuration files of routers is not the responsibility / scope of VINDI; 1.2.3 - The CDE does not have any wireless network connected to it; 1.3.7 - VINDI does not store CHD in its system components.
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2.1.1 - The CDE does not have any wireless network connected to it; 2.6 - VINDI is not a shared hosting provider.
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3.4.1 - No disk encryption in use.
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	4.1.1 - The CDE does not have any wireless network connected to it; 4.2 - VINDI does not transmits cardholder data unencrypted over public or open networks.
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 6:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 8:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	8.1.5 - VINDI does not enable suppliers account for remote access to your environment; 8.5.1 - VINDI is not a Service Provider;

				8.7 - VINDI does not store CHD in its system components.
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	9.5.1, 9.6.x, 9.7.x, 9.8 - VINDI does not store cardholder data in its system components; 9.9.x - VINDI captures cardholder data only from web services.
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 11:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 12:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	12.9 - VINDI is not a shared service provider.
Appendix A1:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	VINDI does not perform shared hosting functions.
Appendix A2:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	VINDI does not use SSL and early TLS in your environment.

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:	<i>May 28th, 2018</i>	
Have compensating controls been used to meet any requirement in the ROC?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the ROC identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Were any requirements not tested?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the ROC 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 the ROC dated **May 28th, 2018**.

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 *VINDI TECNOLOGIA E MARKETING S/A* 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 _____ has not demonstrated full compliance with the PCI DSS.
Target Date for Compliance: N/A
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 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 3.2, 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.

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 *Trustwave Inc.*

Part 3b. Service Provider Attestation



Signature of Service Provider Executive Officer ↑

Date: **May 29th, 2018**

Service Provider Executive Officer Name: **Wagner Narde**

Title: **CTO**

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

If a QSA was involved or assisted with this assessment, describe the role performed: *Project manager and Lead Assessor*



Signature of Duly Authorized Officer of QSA Company ↑

Date: *May 29th, 2018*

Duly Authorized Officer Name: **Paulo Rogério de Aguiar Poi**

QSA Company: *Cipher S/A*

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*

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 the applicable 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 checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<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"/>	
10	Track and monitor all access to network resources and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<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"/>	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

