



# **Payment Card Industry Data Security Standard**

---

## **Attestation of Compliance for Self-Assessment Questionnaire D for Service Providers**

**For use with PCI DSS Version 4.0.1**

Revision 1

Publication Date: December 2024



## Section 1: Assessment Information

### Instructions for Submission

This document must be completed as a declaration of the results of the entity's self-assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures*. Complete all sections: The entity is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which the Attestation of Compliance (AOC) will be submitted for reporting and submission procedures.

This AOC reflects the results documented in an associated Self-Assessment Questionnaire (SAQ).

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Self-Assessment Questionnaire.

Part 1. Contact Information	
Part 1a. Assessed Entity	
Company name:	Headhunter Systems Limited and Graduway Inc.
DBA (doing business as):	Gravyty
Company mailing address:	2815 Elliott Avenue Suite 201
Company main website:	https://gravyty.com
Company contact name:	Rishi Patel
Company contact title:	CFO
Contact phone number:	+1 978 522 4335
Contact e-mail address:	info@gravyty.com
Part 1b. Assessor	
Provide the following information for all assessors involved in the assessment. If there was no assessor for a given assessor type, enter Not Applicable.	
PCI SSC Internal Security Assessor(s)	
ISA name(s):	Not Applicable
Qualified Security Assessor	
Company name:	Marcum RAS, LLC dba CBIZ RAS
Company mailing address:	201 E Kennedy Blvd #1500, Tampa, FL 33602
Company website:	https://www.cbiz.com/
Lead Assessor Name:	Christopher Shaffer
Assessor phone number:	(214) 276 1599
Assessor e-mail address:	christopher.shaffer@cbiz.com
Assessor certificate number:	204-508



Part 2. Executive Summary

Part 2a. Scope Verification

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

Name of service(s) assessed: Advance cloud based fundraising application.		
Type of service(s) assessed:		
<b>Hosting Provider:</b> <input checked="" type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web-hosting services <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Multi-Tenant Service Provider <input type="checkbox"/> Other Hosting (specify):	<b>Managed Services:</b> <input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	<b>Payment Processing:</b> <input type="checkbox"/> POI / card present <input checked="" type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (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):		

**Note:** These categories are provided for assistance only and are not intended to limit or predetermine an entity’s service description. If these categories do not apply to the assessed service, complete “Others.” If it is not clear whether a category could apply to the assessed service, consult with the entity(ies) to which this AOC will be submitted.



## Part 2. Executive Summary *(continued)*

### 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** (select all that apply):

Name of service(s) not assessed: Not Applicable

Type of service(s) not assessed:

Hosting Provider:	Managed Services:	Payment Processing:
<input type="checkbox"/> Applications / software	<input type="checkbox"/> Systems security services	<input type="checkbox"/> POI / 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-hosting services		
<input type="checkbox"/> Security services		
<input type="checkbox"/> 3-D Secure Hosting Provider		
<input type="checkbox"/> Multi-Tenant Service 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:

### Part 2b. Description of Role with Payment Cards

Describe how the business stores, processes, and/or transmits account data.	The organization provides a cloud based fundraising application that uses external payment processors integrated into their website using iframe redirection to facilitate payment processing functions for its clients using PCI DSS validated third party providers.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	The organization hosts a fundraising application that utilizes iFrames for inclusion of payment processing pages from multiple payment processors to facilitate payment functionality for its clients.
Describe system components that could impact the security of account data.	Systems that could impact the security of the account data include the server infrastructure supporting the application and the application which uses PCI-DSS validated service provider technology to capture account data.



Part 2. Executive Summary (continued)

Part 2c. Description of Payment Card Environment

<p>Provide a <b>high-level</b> description of the environment covered by this assessment.</p> <p><i>For example:</i></p> <ul style="list-style-type: none"><li>• <i>Connections into and out of the cardholder data environment (CDE).</i></li><li>• <i>Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.</i></li><li>• <i>System components that could impact the security of account data.</i></li></ul>	<p>Advance is a cloud based software application and the sole application within scope of this assessment. Payment integration completed via PCI compliant integration with Spreedly, Stripe, BBMS, and Braintree payment processor and payment services via an iframe redirection from their fundraising site. No POS devices are utilized or within scope of implementation. The fundrasinign application is hosted using AWS infrastructure as as service. All processing of cardholder data is entirely outsourced to PCI DSS validated third-party service providers.</p>
<p>Indicate whether the environment includes segmentation to reduce the scope of the assessment.</p> <p><i>(Refer to “Segmentation” section of PCI DSS for guidance on segmentation.)</i></p>	<p><input type="checkbox"/> Yes   <input checked="" type="checkbox"/> No</p>

Part 2d. In-Scope Locations/Facilities

List all types of physical locations/facilities—for example, corporate offices, data centers, call centers, and mail rooms—in scope for the PCI DSS assessment.

Facility Type	Total number of locations (How many locations of this type are in scope)	Location(s) of facility (city, country)
<i>Example: Data centers</i>	3	<i>Boston, MA, USA</i>
AWS (data center)	1	USA



**Part 2. Executive Summary** *(continued)*



Part 2e. PCI SSC Validated Products and Solutions

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions\*?

☐ Yes    ☒ No

Provide the following information regarding each item the entity uses from PCI SSC’s Lists of Validated Products and Solutions.

Name of PCI SSC validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which product or solution was validated	PCI SSC listing reference number	Expiry date of listing (YYYY-MM-DD)

\* For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components, appearing on the PCI SSC website ([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org))—for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions, and Mobile Payments on COTS (MPoC) products.



**Part 2. Executive Summary** *(continued)*





Part 2f. Third-Party Service Providers

For the services being validated, does the entity have relationships with one or more third-party service providers that:

<ul style="list-style-type: none"><li>Store, process, or transmit account data on the entity’s behalf (for example, payment gateways, payment processors, payment service providers (PSPs), and off-site storage)</li></ul>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
<ul style="list-style-type: none"><li>Manage system components included in the scope of the entity’s PCI DSS assessment—for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting services, and IaaS, PaaS, SaaS, and FaaS cloud providers.</li></ul>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
<ul style="list-style-type: none"><li>Could impact the security of the entity’s CDE—for example, vendors providing support via remote access, and/or bespoke software developers.</li></ul>	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

If Yes:

Name of service provider:	Description of service(s) provided:
Spreadly	Payment Processor
Stripe	Payment Processor
BBMS	Payment Processor
Braintree	Payment Processor
AWS	Infrastructure as a Service

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



Part 2. Executive Summary (continued)

Part 2g. Summary of Assessment

(SAQ Section 2 and related appendices)

Indicate below all responses provided within each principal PCI DSS requirement.  
For all requirements identified as either “Not Applicable” or “Not Tested,” complete the “Justification for Approach” table below.

**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:

PCI DSS Requirement	Requirement Responses				
	More than one response may be selected for a given requirement. Indicate all responses that apply.				
	In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
Requirement 1:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 2:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 3:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 6:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 8:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 9:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 11:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 12:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Justification for Approach



For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	3.2.1, 3.3.3, 3.4.2, 3.5.1.1, 3.5.1.2, 4.2.1.1, 5.2.3.1, 5.3.2.1, 5.3.3, 5.4.1, 6.3.2, 6.4.2, 6.4.3, 7.2.4-7.2.5.1, 8.3.6, 8.4.2, 8.5.1, 8.6.x, 9.5.1.2.1, 10.4.1.1, 10.4.2.1, 10.7.2, 11.3.1.x, 11.5.1.1, 11.6.1, 12.3.x, 12.5.2.1, 12.5.3, 12.6.2, 12.6.3.x, 12.10.4.1, 12.10.7 - This requirement is not currently required to be in place and considered for a PCI DSS assessment until after March 31, 2025. As such, the QSA did not review or test for this PCI DSS assessment. 9.4.x - Gravyty does not physically store CHD. 9.5.x - Gravyty does not utilized POI devices. 11.4.7 - Gravyty is not a multi-tenant service provider. A1.x - Gravyty is not a multi-tenant hosting provider. A2.x - Gravyty does not use any POS/POI devices with SSL and/or early TLS.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	



## Section 2: Self-Assessment Questionnaire D for Service Providers

Self-assessment completion date:	2/27/2025
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 (Self-assessment completion date 2/27/2025).

Indicate below whether a full or partial PCI DSS assessment was completed:

- ☒ **Full** – All requirements have been assessed therefore no requirements were marked as Not Tested in the SAQ.
- ☐ **Partial** – One or more requirements have not been assessed and were therefore marked as Not Tested in the SAQ. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the SAQ D noted above, each signatory identified in any of Parts 3b–3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document.

Select one:

☒ **Compliant:** All sections of the PCI DSS SAQ are complete, and all assessed requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall **COMPLIANT** rating; thereby *Headhunter Systems Limited - Graduway Inc.* has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not Tested above.

☐ **Non-Compliant:** Not all sections of the PCI DSS SAQ are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating, thereby *(Service Provider Company Name)* has not demonstrated compliance with the PCI DSS requirements included in this SAQ.  
**Target Date** for Compliance: YYYY-MM-DD  
An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted *before completing Part 4.*

☐ **Compliant but with Legal exception:** One or more assessed requirements in the PCI DSS SAQ are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Service Provider Company Name)* has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not Tested above or as Not in Place due to a legal restriction.  
This option requires additional review from the entity to which this AOC will be submitted. *If selected, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement from being met



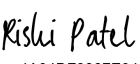
### Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:

(Select all that apply)


<input checked="" type="checkbox"/>	PCI DSS Self-Assessment Questionnaire D, Version 4.0.1, 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 the entity's assessment in all material respects.
<input checked="" type="checkbox"/>	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

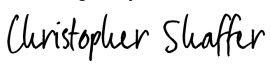
### Part 3b. Service Provider Attestation

DocuSigned by:  4A04DF0387E0489...	
Signature of Service Provider Executive Officer ↑	Date: 3/14/2025
Service Provider Executive Officer Name: <b>Rishi Patel</b>	Title: <b>CFO</b>

### Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this assessment, indicate the role performed:	<input checked="" type="checkbox"/> QSA performed testing procedures.
	<input type="checkbox"/> QSA provided other assistance. If selected, describe all role(s) performed:

DocuSigned by:  346B24B230CB4CA...	
Signature of Lead QSA ↑	Date: 3/14/2025
Lead QSA Name: <b>Christopher Shaffer</b>	

DocuSigned by:  346B24B230CB4CA...	
Signature of Duly Authorized Officer of QSA Company ↑	Date: 3/14/2025
Duly Authorized Officer Name: <b>Christopher Shaffer</b>	QSA Company: <b>Marcum RAS, LLC dba CBIZ RAS</b>

### Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this assessment, indicate the role performed:	<input type="checkbox"/> ISA(s) performed testing procedures.
	<input type="checkbox"/> ISA(s) provided other assistance. If selected, describe all role(s) performed:



## Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has a Non-Compliant status noted in Section 3.

If asked to complete this section, select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement below. For any “No” responses, include the date the entity expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

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 network security controls	<input type="checkbox"/>	<input type="checkbox"/>	
2	Apply secure configurations to all system components	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored account data	<input type="checkbox"/>	<input type="checkbox"/>	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems and networks from malicious software	<input type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and software	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to system components and cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identify users 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	Log and monitor all access to system components and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Test security systems and networks regularly	<input type="checkbox"/>	<input type="checkbox"/>	
12	Support information security with organizational policies and programs	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	<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"/>	

**Note:** The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance-accepting organization to ensure that this form is acceptable in its program. For more information about PCI SSC and our stakeholder community please visit: [https://www.pcisecuritystandards.org/about\\_us/](https://www.pcisecuritystandards.org/about_us/).