Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Self-Assessment Questionnaire D – Service Providers

For use with PCI DSS Version 3.2.1

Revision 2

September 2022

Document Changes

Date	PCI DSS Version	SAQ Revision	Description
September 2022	3.2.1	2.0	Updated to reflect the inclusion of UnionPay as a Participating Payment Brand.

Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the service provider's self-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:	Ticketsolve Limited	DBA (doing business as):	Ticketsolve
Contact Name:	Sean Hanly	Title:	Chief Executive Officer (CEO)
Telephone:	+34 (93) 894 7048	E-mail:	shanly@ticketsolve.com
Business Address:	29, Guinness Enterprise Centre, Taylor's Lane	City:	DUBLIN
State/Province:	Dublin Region	Country: Republic of Ireland	Zip: 8
URL:	www.ticketsolve.com		

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

Company Name:	3B Data Security		
Lead QSA Contact Name:	James Boughey	Title:	Information Security Team Manager
Telephone:	+44 (0) 1223 298 333	E-mail:	James.Boughey@3BDataSecurity.com
Business Address:	Unit D, South Cambridge Business Park	City:	Cambridge
State/Province:	Cambridgeshire	Country: England	Zip: CB22 3JH
URL:	www.3BDataSecurity.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:	Ticketsolve Ticketing Platform

Type of service(s) assessed:

Hosting Provider:	**Managed Services (specify):**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POS / card present
☐ Hardware	☐ IT support	☒ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☒ Other services (specify):	☐ Other processing (specify):
☒ Web	Ecommerce platform	
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Shared Hosting Provider		
☐ Other Hosting (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:**
☐ Applications / software	☐ Systems security services	☐ POS / card present
☐ Hardware	☐ IT support	☐ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Shared Hosting Provider		
☐ Other Hosting (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):		

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.	Ticketsolve Limited provide a white labelled site which includes a checkout process to purchase tickets from the website. Once the clients' customers have selected the tickets they require, a fully hosted payment page rendered via an iframe is used for the customer to enter payment details.
	All elements of the fully hosted payment page is delivered to the consumer's browser directly from a PCI DSS validated third-party service provider. Therefore, Ticketsolve does not store, process, or transmit cardholder data on their infrastructure or systems.
	In most cases each client will use their own merchant ID (MID) which is configured for them on the Ticketsolve system. However, for a small number of customers Ticketsolve Limited uses their own MID and credits purchases back to their clients. This merchant channel undergoes its own separate assessment and is not included wihtin the scope of this assessment.

Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Ticketsolve Limited does not store, process or transmit any cardholder data within the booking application. All cardholder data is captured directly using a fully hosted payment page rendered via an iframe is used for the customer to enter payment details.

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*
Head office	1	Dublin, ROI.

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)
N/A	N/A	N/A	☐ Yes ☒ No	N/A
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ 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.*	The environment covered by this assessment is as follows: • Coding of the payment page. • Hosting environment and services. • Connections into and out of the cardholder data environment. • Review of services and infrastructure provided by third party service providers.

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 have a relationship with a Qualified Integrator Reseller (QIR) for the purpose of the services being validated?	☐ Yes ☒ No

If Yes:

Name of QIR Company:	N/A
QIR Individual Name:	N/A
Description of services provided by QIR:	N/A

Part 2f. Third-Party Service Providers (Continued)

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?	☒ Yes ☐ No

If Yes:

Name of service provider:	Description of services provided:
Global Payments (Realex)	Payment Service Provider (PSP)
Amazon Web Services	Cloud hosting services.

***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 were assessed for that Requirement, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the SAQ.
- Partial – One or more sub-requirements of that Requirement were marked as "Not Tested" or "Not Applicable" in the SAQ.
- None – All sub-requirements of that Requirement were marked as "Not Tested" and/or "Not Applicable" in the SAQ.

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 SAQ
- 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:	Ticketsolve Ticketing Platform

PCI DSS Requirement	Details of Requirements Assessed			
	Full	Partial	None	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	☐	☐	☒	**The Ticketsolve platform has been designed specifically to meet the eligibility criteria of Self-Assessment Questionnaire A (SAQ A) therefore this requirement was deemed to be notapplicable.**
Requirement 2:	☐	☒	☐	**The Ticketsolve platform has been designed specifically to meet the eligibility criteria of Self-Assessment Questionnaire A (SAQ A) therefore only requirements 2.1.a and 2.1.b were included in this assessment.**
Requirement 3:	☐	☐	☒	**The Ticketsolve platform has been designed specifically to meet the eligibility criteria of Self-Assessment Questionnaire A (SAQ A) therefore this requirement was deemed to be notapplicable.**
Requirement 4:	☐	☐	☒	**The Ticketsolve platform has been designed specifically to meet the eligibility criteria of Self-Assessment Questionnaire A (SAQ A) therefore this requirement was deemed to be notapplicable.**
Requirement 5:	☐	☐	☒	**The Ticketsolve platform has been designed specifically to meet the eligibility criteria of Self-Assessment Questionnaire A (SAQ A) therefore this requirement was deemed to be notapplicable.**

Requirement 6:	☒	☐	☐	**The Ticketsolve platform has been designed specifically to meet the eligibility criteria of Self-Assessment Questionnaire A (SAQ A) therefore only requirements 6.2.a and 6.2.b were included in this assessment.**
Requirement 7:	☐	☐	☒	**The Ticketsolve platform has been designed specifically to meet the eligibility criteria of Self-Assessment Questionnaire A (SAQ A) therefore this requirement was deemed to be notapplicable.**
Requirement 8:	☐	☒	☐	**The Ticketsolve platform has been designed specifically to meet the eligibility criteria of Self-Assessment Questionnaire A (SAQ A) therefore only requirements 8.1.1, 8.1.3, 8.2, 8.2.3.a and 8.5 were included in this assessment.**
Requirement 9:	☐	☒	☐	**The Ticketsolve platform has been designed specifically to meet the eligibility criteria of Self-Assessment Questionnaire A (SAQ A) therefore only requirements 9.5, 9.6, 9.6.1, 9.6.2, 9.6.3, 9.7, 9.8.a and 9.8.c, 9.8.1.a and 9.8.1.b were included in this assessment.**
Requirement 10:	☐	☐	☒	**The Ticketsolve platform has been designed specifically to meet the eligibility criteria of Self-Assessment Questionnaire A (SAQ A) therefore this requirement was deemed to be notapplicable.**
Requirement 11:	☐	☐	☒	**The Ticketsolve platform has been designed specifically to meet the eligibility criteria of Self-Assessment Questionnaire A (SAQ A) therefore this requirement was deemed to be notapplicable.**
Requirement 12:	☐	☒	☐	**The Ticketsolve platform has been designed specifically to meet the eligibility criteria of Self-Assessment Questionnaire A (SAQ A) and service provider specific requirements 12.4.1.a, 12.4.1.b, 12.8, 12.8.1, 12.8.2, 12.8.3, 12.8.4, 12.8.5, 12.9 and 12.10.1 were included in this assessment.**
Appendix A1:	☐	☐	☒	**Not Applicable - Ticketsolve Limited do not operate as a shared hosting provider.**
Appendix A2:	☐	☐	☒	**Not Applicable - Ticketsolve Limited web applications do not utilise SSL or early TLS in the environment.**

Section 2: Self-Assessment Questionnaire D – Service Providers

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:	4th August 2023
Have compensating controls been used to meet any requirement in the SAQ?	☒ Yes ☐ No
Were any requirements in the SAQ identified as being not applicable (N/A)?	☒ Yes ☐ No
Were any requirements in the SAQ identified as being not tested?	☒ Yes ☐ No
Were any requirements in the SAQ 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 SAQ D (Section 2), dated *4th August 2023*.

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):**

☒	**Compliant:** All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *Ticketsolve Limited* has demonstrated full compliance with the PCI DSS.
☐	**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 *(Service Provide 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 the payment brand(s) before completing Part 4.*
☐	**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. *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)

☒	PCI DSS Self-Assessment Questionnaire D, Version *3.2.1*, was completed according to the instructions therein.
☒	All information within the above-referenced SAQ 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 data[1], CAV2, CVC2, CVN2, CVV2, or CID 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 *(ASV Name)*

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑ *(signature)*	*Date:* **August 9th, 2023**
Service Provider Executive Officer Name: **Sean Hanly**	*Title:* **Chief Executive Officer (CEO)**

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

If a QSA was involved or assisted with this assessment, describe the role performed:	Scope verification, PCI Control Validation, Final Assessment and RoC reporting.

jboughey

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* **August 10th, 2023**
Duly Authorized Officer Name: **James Boughey**	*QSA Company:* **3B Data Security**

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	☐	☐	
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 A1	Additional PCI DSS Requirements for Shared Hosting Providers	☐	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections.	☐	☐	