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

July 2018

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:	Ultracomms		DBA (doing business as):	N/A	
Contact Name:	Dan Davies		Title:	Infrastructure Manager	
Telephone:	02031671135		E-mail:	dan.davies@ultracomms.com	
Business Address:	Compass House, North Harbour Business Park		City:	Portsmouth	
State/Province:	Hampshire	Country:	UK	Zip:	PO6 4PS
URL:	www.ultracomms.com				
Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	Nettitude Ltd.				
Lead QSA Contact Name:	Mike Somers		Title:	Information Security Consultant	
Telephone:	+44 (0) 7943 982926		E-mail:	msomers@nettitude.com	
Business Address:	1 Jephson Court, Tancred Close		City:	Leamington Spa	
State/Province:	Warwickshire	Country:	UK	Zip:	CV31 3RZ
URL:	https://www.nettitude.com/uk				

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:	Ultra Call Management System (UCMS)

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		Contact Centre/ Call Center solution provider that does managed telephone based payments.
☐ 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:	

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:	

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	The Ultra Call Management System (UCMS) is hosted in multiple Data Centre's and provides off premise telephone call management services across the UK. A Contact Centre agent using the UCMS Call Bar desktop application can process card-not-present payments over the telephone by asking their customer to enter payment card information, with their standard telephone keypad buttons, while they are still talking which results in a more personal and reassuring interaction. A fully automated service is also provided for self service payments for when agents are unavailable. The keypad button tones are screened and turned into data within the Ultra Communications off premise solution, and passed to the clients preferred payment service provider (PSP) for authorisation. As a result, payment card details are never processed by the Contact Centre
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	N/A

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*
Data centre	2 1	London, UK Studley, UK

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)
			☐ Yes ☐ No	
			☐ 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.*

People

Development – Development team responsible for the development, maintenance and updates of the Ultra UCMS platform. System Administration – Team responsible for the implementation, administration and maintenance of all CDE and Non CDE devices. This includes all Firewalls, network devices, servers, workstations and physical security access requests. Administrators are also responsible for security testing such as internal, vulnerability scanning, external ASV scan schedules. Physical Security – Third party organisations responsible for the security and maintenance of Data Centre facilities: access control, facility monitoring etc. of the security of Data Center Human Resources -

	Recruits for all advertised vacancies within the Ultra Home offices, sourcing candidates, attending interviews, offering roles and the associated paperwork to accompany this. Human Resources are also responsible for the monitoring of training activities. Processes Payment Channels – Ultra UCMS system processes CardNot-Present authorisation requests for merchant's Contact Centers. All authorisation requests are provisioned through off-premise telephony hardware using DTMF technology whilst the customers are on a telephone session. Payment Functions – Ultra managed payment switching application and hardware located within Ultra third party managed Data Centers which handle the storage and transmission of CHD for the purposes of payment authorisation were observed during the on-site visits. Physical Access Controls - Technology and formally documented processes for controlling access, badging,monitoring and authorisation of personnel accessing sensitive areas within the three third party managed Data Centers. Vulnerability Management – Ultra engaged a third party vendor (Coalfire Labs) to perform their ASV scans and penetration tests. Host Based IPS – Ultra utilized a host based intrusion protection solution for critical points within the CDE. Technologies Networking – Firewalls and switches used to segment the CDE and Non-CDE environments from each. Ultra does not utilise routers in their environment. Server Hardware – Server hardware used to support varying server roles, virtualisation and provisioning of storage within the CDE. Virtualisation Technology – virtualisation technologies used for the provisioning of virtual servers supporting the CDE. Workstations – Administrator workstation used to connect to the Isolated CDE environments within the three Data Centers using VPN and TwoFactor (2FA) authentication.
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:	
QIR Individual Name:	
Description of services provided by QIR:	

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:**
Realex	Payment Services Provider
WorldPay (UK) Ltd	Payment Services Provider
SagePay	Payment Services Provider
Cybersource	Payment Services Provider
Barclaycard SmartPay	Payment Services Provider
Barclaycard EPDQ	Payment Services Provider
PXP	Payment Services Provider
FIRST DATA	Payment Services 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 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:	Ultra Communications Call Management System (UCMS)

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:	☐	☒	☐	**1.2.2 – There are no routers within the Cardholder Data Environment.** **1.2.3 – There are no wireless networks connected to the in-scope environment.**
Requirement 2:	☐	☒	☐	**2.1.1 – There are no wireless networks connected to the in-scope environment.** **2.6 – Ultra Communications is not a shared hosting provider.**
Requirement 3:	☐	☒	☐	**3.2 – Ultra Communications is not an issuer and does not support issuing service.** **3.3 – Ultra Communications does not facilitate the display of CHD.** **3.4.1 – Ultra Communications does not utilise disk encryption technologies.** **3.6 – Ultra Communications does not distribute cryptographic keys.** **3.6.2 – Ultra Communications does not distribute cryptographic keys.** **3.6.6 – Ultra Communications does not utilise manual clear-text cryptographic keymanagement operations.** **3.6.7 – Ultra Communications does not manage the substitution of cryptographic keys.**

				3.6.8 – Ultra Communications does not manage cryptographic keys on behalf of others.
Requirement 4:	☐	☒	☐	**4.1.1 - Wireless networks are not permitted** **4.2 - End-user messaging technogies are not used within the UCMS**
Requirement 5:	☒	☐	☐	
Requirement 6:	☒	☐	☐	
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	**8.1.6.b – Ultra Communications does not provide nonconsumer customer user accounts.** **8.2.1.b, 8.2.3.b, 8.2.4.b, 8.2.5.b – All nonconsumer customer user accounts requirements are configurable by the customer.** **8.5.1 – Ultra Communications does not have remote access to customer premises.** **8.7 – Ultra Communications do not have any databases containing CHD.**
Requirement 9:	☐	☒	☐	**9.5 – Ultra Communications does not store CHD.** **9.6 – Ultra Communications does not store CHD.** **9.7 – Ultra Communications does not store CHD.** **9.8 – Ultra Communications does not store CHD.** **9.9 – There are no POS devices in scope for this assessment.**
Requirement 10:	☒	☐	☐	
Requirement 11:	☐	☒	☐	**11.1 – There are no wireless networks connected to the in-scope environment.** **11.3.4 – Ultra Communications does not use segmentation to isolate the CDE from other networks.**
Requirement 12:	☒	☐	☐	
Appendix A1:	☐	☐	☒	**Ultra Communications is not a shared hosting provider**
Appendix A2:	☐	☐	☒	**No Card Present Payment systems in use**

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:	12/08/2019	
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 *12/08/2019.*

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):***

☒	**Compliant:** All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *Ultra Comms* 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 *v3.2.1*, 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, CID, or CVV2 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 *Nettitude Ltd and Coalfire.*

Part 3b. Service Provider Attestation

Dan Davies

Signature of Service Provider Executive Officer ↑	*Date:* 15/08/2019
Service Provider Executive Officer Name: Dan Davies	*Title:* Infrastructure Manager

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

If a QSA was involved or assisted with this assessment, describe the role performed:	QSA confirmed through; interviews with staff, reviews of documentation and network configuration the scope of Ultra Comms environment. The QSA also reviewed the completed SAQ and validated it was accurate. A limited technical review was completed which was constrained to firewall configurations and technical processes.

Michael W Somers

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* **12/08/2019**
Duly Authorized Officer Name: **Mike Somers**	*QSA Company:* **Nettitude Ltd.**

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:	

[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.	☐	☐