PCI Security Standards Council

Payment Card Industry (PCI) Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

June 2018

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:	Creditcall Limited		DBA (doing business as):	N/A	
Contact Name:	Jeremy Gumbley		Title:	Chief Security Officer	
Telephone:	+44(0)117 930 4455		E-mail:	Jeremy.Gumbley@nmi.com	
Business Address:	Merchants House North, Wapping Road		City:	Bristol	
State/Province:	England	Country:	United Kingdom	Zip:	BS1 4RW
URL:	https://www.creditcall.com				

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

Company Name:	Foregenix Limited				
Lead QSA Contact Name:	Dalitso Phiri		Title:	Principal Security Consultant	
Telephone:	+44 845 309 6232		E-mail:	dphiri@foregenix.com	
Business Address:	1st Floor, 8-9 High Street		City:	Marlborough	
State/Province:	Wiltshire	Country:	United Kingdom	Zip:	SN8 1AA
URL:	http://www.foregenix.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:	CardEase, eKashu and WebMIS
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:	Not Applicable	
Type of service(s) not 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):		
Provide a brief explanation why any checked services were not included in the assessment:	Not Applicable	

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Creditcall Limited is a Level 1 Payment Service Provider that facilitates the processing of incoming transactions for authorisation from merchant clients. Creditcall receives both Card Present and Card Not Present transaction authorisation request for processing form client merchant agents' networks using e-commerce and PED payment channels. Creditcall receives CHD from merchant client's networks via HTTPS interfaces. In response to vulnerabilities identified with using SHA-1 and early TLS implementations, Creditcall has upgraded the security software and configuration to use HTTPS connections that support TLS v1.2 with a minimum AES128-bit key length. Creditcall maintains a separate legacy platform that supports clients that can only transmit CHD using TLS v1.0 and SHA-1 certificates on their devices. The interfaces used to support client merchants are configured to use TLS v1.0 so Merchant Agents can commit their transactions for processing. Creditcall has performed risk assessment and communicating deadlines to their merchants to commit to TLS v1.2 with a minimum AES 128-bit key length upgrade before 30 Dec 2019 as the final deadline before support for lower variants and insecure TLS version are withdrawn and no longer supported for connection to Creditcall for transactional processing. Creditcall have upgraded all their systems with an exception to one system used to support legacy software being used by their clients. Creditcall uses proprietary CardEase protocols to receive card present or not present transactions from its merchant clients and agents and supports real-time transactions or batch files for bulk processing. These channels of data are transmitted directly to Acquirers for authorisation and settlement via the following channels: CardEaseXML/ChipDNA Direct which is Creditcall's payment protocol hosted on the CardEase V2 platform architecture. The application uses requests and responses that support XML encapsulated using TLS v1.2 (RSA 2048 bit). eKashu is the e-commerce payment processing service that uses TLS and is used to perform transaction authorisation for card-not-present transactions. A70 is an application that provides transaction authorisation and settlement services for CardEase platform. Creditcall maintains and retains records of transaction history [redacted]. The CHD (PAN first six (6) and last four (4) including

	expiry data [redacted] is encrypted with AES 256-bit key. The stored data is subjected to data retention periods of 12 months before its automatically purged from the Database. Creditcall also provides its clients with a web portal called WebMIS. Customers use the portal to view reports regarding for transaction volumes. The portal is also used to address queries such as settlement and refunds for users with authorised access. All CHD data transactions involving process of sensitive authentication data in the VRAM and are not stored or committed to any media for short or long-term storage. Creditcall's environment also hosts a Point to Point Encryption (P2PE) solution called 'Creditcall P2PE Solution.' This solution is used to encrypt data at the POI devices using DUKPT 3DES 128-bits. The encrypted data from POI devices on client or merchant agent site is transmitted to Creditcall and processed using the is CardEase application. All transactions are checked and validated by the load balancer before the encrypted CHD data is forwarded to XML server for decryption and processing. The decryption is handled by the Crypto Server which uses an API call request to the HSMs. The data is then returned to the Crypto Server. Clear text account data is sent back to the XML server which stores the transaction [redacted] storing only the first 6 and last 4 digits of the PAN, whilst also forwarding the data to the acquirers and processors for authorisation. Creditcall uses an IPsec VPN or TLS 1.2 to transmit cardholder data depending upon the acquirer's supported channels.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Creditcall receives cardholder data for processing from Merchant Agents via VPN and TLS encrypted channels and transmits the captured cardholder data to partner acquires and payment service providers for authorisation and settlements purposes. Creditcall also maintains and stores cardholder data PAN, that is used for reporting purposes. PAN is stored in a database within a tablespace that is encrypted using AES 256-bit key.

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):
Corporate Office	1	Bristol, United Kingdom
Corporate Office	1	Creditcall New York,315 W 36th Street,New York,NY 10018,United States
Data Centre	5	[redacted]

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)
CardEase	1.3	Creditcall	☐ Yes ☒ No	Not Applicable

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 Creditcall environment is segmented between the corporate and cardholder data processing environments. The corporate environment located at Creditcall's Office in Bristol and is the location where the administrative, operations and development environment are hosted. The Corporate environment does not receive, process or transmit cardholder data. Creditcall uses dedicated and third-party managed data center facilities to host its CDE; [redacted] All virtual access to the data centre environment can only be achieved using VPN with Jump host that supports multi-factor authentication. The data centre environments are firewalled and contain multiple dedicated network zones used to host application and management servers. This allows Creditcall to apply granular role-based access to its environment and only users with a need to know are granted permission to access the facility both physically and virtually. Technologies included within the assessment included:

	Firewalls Loadbalancers Encryption Authentication Databases Management tools FIM, IDS Virtualizations Servers, Routers, Switches Anti-virus and patching

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:	Not Applicable
QIR Individual Name:	Not Applicable
Description of services provided by QIR:	Not Applicable

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:**
[redacted]	Fraud Detection Service
[redacted]	Data Center Hosting Service Provider
[redacted]	Fraud Detection Service
[redacted]	Offsite Media Storage Service Provider
[redacted]	Data Center Hosting Service Provider
[redacted]	Data Center Hosting Service Provider
[redacted]	Data Center Hosting Service Provider
[redacted]	Transaction Authorisation and Settlement 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 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:	CardEase 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:	☐	☒	☐	**1.4 Not Applicable – Creditcall does not allow or facilitate direct access connection to the CDE from mobile computers.**
Requirement 2:	☐	☒	☐	**2.1.1 Wireless not connected to the CDE**
Requirement 3:	☒	☐	☐	**3.4.1 Not Applicable – Creditcall does not use disk encryption to protect cardholder data.**
Requirement 4:	☐	☒	☐	**4.1.1 Not Applicable – Creditcall does not host or maintain wireless networks within the CDE.** **4.2 Not Applicable – Creditcall does not used end-user messaging systems or technologies to send cardholder data.**
Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	**6.4.6 Not applicable – No Significant Changes have been made**
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	**8.1.5 Not applicable – Creditcall does not allow or facilitate vendor access to cardholder data.**

				8.1.6.b Not Applicable – Creditcall does not provide or facilitate non-consumer user access to cardholder data. 8.2.3.b Not Applicable – Creditcall does not provide or facilitate non-consumer user access to cardholder data. 8.2.4.b Not Applicable – Creditcall does not provide or facilitate non-consumer user access to cardholder data. 8.2.5.b Not Applicable – Creditcall does not provide or facilitate non-consumer user access to cardholder data. 8.2.6.b Not Applicable – Creditcall does not provide or facilitate third-party or vendor access to cardholder data. 8.5.1 Not Applicable – Creditcall does not have remote access to consumer environments.
Requirement 9:	□	☒	□	9.9 Not Applicable – Creditcall does not maintain or manage devices that physically capture cardholder data.
Requirement 10:	☒	□	□	
Requirement 11:	☒	□	□	
Requirement 12:	☒	□	□	
Appendix A1:	□	□	☒	Not Applicable – Creditcall is not a shared hosting provider.
Appendix A2:	☒	□	□	

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:	*29 March 2019*	
Have compensating controls been used to meet any requirement in the ROC?	☒ Yes	☐ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes	☐ No
Were any requirements not tested?	☐ Yes	☒ No
Were any requirements in the ROC 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 the ROC dated *29 March 2019.*

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 *Creditcall Limited* 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 *(Service Provider 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 "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 *3.2.1* 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 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 *Qualys*

Part 3b. Service Provider Attestation	
Signature of Service Provider Executive Officer ↑	*Date:* **29 March 2019**
Service Provider Executive Officer Name: **Jeremy Gumbley**	*Title:* **Chief Security Officer**

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)	
If a QSA was involved or assisted with this assessment, describe the role performed:	*Foregenix provided PCI Gap Assessment and PCI DSS Certification Services. This included the scope validation, interviews and tests, with the output of the results used to write the ROC.*

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* ***29 March 2019***
Duly Authorized Officer Name: **Ariel Ben Harosh**	*QSA Company:* **Foregenix Limited**

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)	
If an ISA(s) If no ISA in the assessment, then simply include Not Applicable here. 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 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	☒	☐	