Payment Card Industry (PCI)

Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.1

March 2015

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:	NCR Corporation		DBA (doing business as):	NCR Connected Payments	
Contact Name:	Juan Piacquadio		Title:	Director IT Global Payments	
ISA Name(s) (if applicable):	N/A		Title:	N/A	
Telephone:	949-330-2109		E-mail:	Juan.Piacquadio@ncr.com	
Business Address:	85 Argonaut Suite 150		City:	Aliso Viejo	
State/Province:	CA	Country:	Orange	Zip:	92656
URL:	www.ncr.com				

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

Company Name:	Coalfire Systems, Inc.				
Lead QSA Contact Name:	Patrick Ibrahim		Title:	Security Consultant	
Telephone:	303-554-6333		E-mail:	PCIQA@coalfire.com	
Business Address:	11000 Westmoor Cir #125,		City:	Westminster,	
State/Province:	CO	Country:	United States	Zip:	80021
URL:	www.Coalfire.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:	NCR Connected Payments	
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.

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:		

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	NCR Connected Payments receives POS information from the client (merchant), then NCR Connected Payment's software encrypts the string using 3DES DUKPT 168 bit encryption, at which point the HSM payShield 9000 encrypts the string with AES 256 bit encryption, and temporarily stores information in a database (while the processor sends the information string to the authorizer), until the transaction is complete at which point, the files are securely deleted and keys are destroyed. Before the information string is stored in the database, it is again encrypted with AES 128 bit encryption. The following databases are used for storing cardholder data: • ServerEPS_Common • ServerEPS_Engine_Active • ServerEPS_Enigne_Resolved • ServerEPS_Engine_Settled For connections between clients and banking entities, either SSL v3 or TLS 1.2 connections are allowed. NCR Connected Payments will process stored and forward batch transactions; however, the information contained within these transactions is not stored within the NCR Connected Payments cardholder data environment. For general transaction processing, payments are routed through NCR Connected Payment's firewalls, allowing only approved traffic, which are then encrypted twice, stored temporarily, sent to the processing entity (via TLS 1.2 or greater, or SSL v3), and upon receipt of approval, the stored information is then purged after an "approval" message is passed to the point of interaction. For PIN/Debit transactions, the process channel is identical, however depending upon the customer's issuer, the information is routed to the respective issuing authority.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Not applicable.

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	1	Aliso Viejo, CA, USA.
Datacenters	3	Tustin, CA, USA Auburn, IN, USA

		Allen, TX, USA

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

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.*	Payment processes: Customers will transmit structured messages which are routed to the appropriate acquirers. NCR Connected Payments accepts the following payment channels: ▪ Card-Present (PAN, expiration date,) ▪ Card-Not-Present (PAN, expiration date, ▪ CVV2/CVC2/CID) ▪ PIN/Debit (PAN, expiration, encrypted PIN block) ▪ Two different types of tokenization are offered incidentally to payment processing, but not separately. ▪ These payment processes pass through the CDE, but all information within the CDE is encrypted in transit, at egress and ingress, as well as at rest in storage. Business functions: Human Resources manages background checks and conducts security awareness training for the personnel who administer the cardholder data environment (CDE). Training is at the time of initial hire, and yearly thereafter. Information Technology: Designs, specifies, builds, manages and troubleshoots the technology that makes up the CDE: ▪ Network management of the firewall, switches and customer connections ▪ Systems administration of the servers and logical access to components of the CDE ▪ Development of custom software to accept customer payment transactions and forward to acquiring banks ▪ Encryption of CHD is enabled by keys that are managed automatically, but backed up by key custodians ▪ Vulnerability management and security monitoring of the CDE connected devices by McAfee Nitro. ▪ Patch management and change management, Gemini is used for change control tickets. ▪ Wireless scanning to identify rogue wireless devices.

	▪ VPN access to CDE via Cisco VPN. The processes identified above include imbedded controls to protect the CDE and the information that passes through it. ▪ Internet connection to receive transactions from customers (leased lines) ▪ Internal network segments (DMZ, trusted, management) to partition the environment and limit risk facilitated by switches, routers and firewalls ▪ Processor connections to send customer transactions and receive status messages provided by the issuer ▪ Customer-side application that encrypts and transmits cardholder data from customer Point of Sale (POS) (facilitated by NCR Connected Payments Software) ▪ VLANs to further enforce and facilitate segmentation ▪ Database systems that temporarily and securely store CHD ▪ McAfee DLP devices and software intended to detect the presence of SAD or CHD and isolate it. ▪ HP Procurve switches used to pass traffic throughout the network. ▪ VPN technology utilizing Cisco VPN for CDE access. ▪ Firewalls used for restricting traffic and controlling access to the CDE. ▪ Web application firewalls ▪ Load balancers Cisco ACE 4710s used to manage traffic ▪ Active Directory for account provisioning. ▪ SFTP server for client level access to reports. ▪ SMTP server for mail. ▪ Logging software for monitoring systems and tracking events. ▪ Microsoft Server for systems operating in the environment. ▪ Proprietary software solutions created by NCR Connected Payments.
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 one or more third-party service providers (for example, 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:	
Type of service provider:	**Description of services provided:**
ACIBashas	Upstream processor
ACIBigY	Upstream processor

ACIBrookshire	Upstream processor
ACIHannaford	Upstream processor
ACIHyVee	Upstream processor
ACIKvat	Upstream processor
ACISuperValu	Upstream processor
ACIWholeFood	Upstream processor
ADS	Upstream processor
BankOfAmerica	Upstream processor
Certegy	Upstream processor
Chase	Upstream processor
Chase-Settlement	Upstream processor
ConcordEPC	Upstream processor
Concord-H&C	Upstream processor
Elavon	Upstream processor
EpicTranz	Upstream processor
FDNashville	Upstream processor
FifthThird	Upstream processor
InComm	Upstream processor
Publix	Upstream processor
RapidConnect	Upstream processor
RBSLynk	Upstream processor
RGA	Upstream processor
RNKBigY	Upstream processor
Shazam	Upstream processor
SoluPay	Upstream processor
SVDot	Upstream processor
TDMS	Upstream processor
TeleCheck	Upstream processor
TGTTandem	Upstream processor
VantivIBM	Upstream processor
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:	NCR Connected Payments			
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: (N/A) No routers in the CDE**
Requirement 2:	☐	☒	☐	**2.1.1: (N/A) No wireless in the CDE** **2.6: (N/A) NCR Connected Payments is not a shared hosting provider.**
Requirement 3:	☐	☒	☐	**3.4.1: (N/A) NCR does not use full disk encryption.**
Requirement 4:	☐	☒	☐	**4.1.1: (N/A) NCR does not transmit CHD over wireless networks** **4.2: (N/A) NCR employees do not have access to unencrypted PAN or CHD, and do not have the ability to send that information over any end user messaging platform.**
Requirement 5:	☒	☐	☐	
Requirement 6:	☒	☐	☐	
Requirement 7:	☒	☐	☐	
Requirement 8:	☒	☐	☐	
Requirement 9:	☐	☒	☐	**9.6.2: (N/A) No media is sent outside the CDE** **9.6.3: (N/A) No media is sent outside the CDE**

				9.7: (N/A) No hardcopy paper CHD is stored **9.9: (N/A) NCR Connected Payments does not have payment capture devices.** **9.9.1: (N/A) NCR Connected Payments does not have payment capture devices.** **9.9.2: (N/A) NCR Connected Payments does not have payment capture devices.** **9.9.3: (N/A) NCR Connected Payments does not have payment capture devices.**
Requirement 10:	☒	☐	☐	
Requirement 11:	☐	☒	☐	**11.1.1: (N/A) NCR does not allow wireless into the CDE nor do they allow connections from wireless networks into the CDE**
Requirement 12:	☒	☐	☐	
Appendix A:	☐	☐	☒	**(N/A) NCR Connected Payments is not a shared hosting provider.**

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:	03/15/2016	
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

Based on the results noted in the ROC dated *03/11/2016*, 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 as of *03/11/2016)*: (***check one):***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby NCR Connected Payments 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 NCR Connected Payments 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
N/A	N/A
N/A	N/A

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 *3.1*, 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 *Coalfire Systems, Inc.*

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	*Date:* 3/15/2016
Service Provider Executive Officer Name: ALOK KUMAR	*Title:* CISO NCR RETAIL

Part 3c. QSA Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	*PCI DSS Validation Services. The Coalfire QSA performed document, configuration, and process reviews in order to determine NCR Corporation's compliance with PCI DSS v.3.1. Additionally the Coalfire QA performed interviews and participated in guided reviews to understand the environment and processes.*

Signature of Duly Authorized Officer of QSA Company ↑	*Date: 03/15/2016*
Duly Authorized Officer Name: Patrick Ibrahim	*QSA Company:* Coalfire Systems, Inc.

Part 3d. ISA Acknowledgement (if applicable)

If an ISA was involved or assisted with this assessment, describe the role performed:	*N/A*

N/A

Signature of ISA ↑	*Date: N/A*
ISA Name: N/A	*Title: 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	☒	☐	