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:	Concur Technologies, Inc.		DBA (doing business as):	Not applicable.	
Contact Name:	Saju Pillai		Title:	Chief Technology Officer	
Telephone:	1.800.401.8412		E-mail:	saju.pillai@sap.com	
Business Address:	601 108th Ave NE #1000		City:	Bellevue	
State/Province:	WA	Country:	Bellevue	Zip:	98004
URL:	https://eu.concursolutions.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	Schellman & Company, LLC				
Lead QSA Contact Name:	Kate Donofrio		Title:	Manager, QSA	
Telephone:	866.254.0000 ext. 212		E-mail:	pcirocs@schellman.com	
Business Address:	4010 W Boy Scout Boulevard, Suite 600		City:	Tampa	
State/Province:	FL	Country:	USA	Zip:	33607
URL:	https://www.schellman.com/pci-dss-validation				

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:	Concur Travel and Expense (CTE)	
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): Facilitate booking and management of travel; Expense management		

***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:	All other Concur Applications and Services	
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:	Concur performs separate PCI DSS assessments for other applications and service offerings.	

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Concur is a wholly owned subsidiary of SAP. Concur Travel and Expense ("CTE") is a Software-as-a-Service (SaaS) solution that provides approval workflow of travel requests, collection of travel data, expense report management, expense reimbursement, invoice management, batch processing of data, and reporting. CTE is made up of the following applications: Travel, Expense, Invoice, Imaging, Workbench, eReceipts, ExpenseIt, TripIT Cognos/Analytics, and Risk Messaging. Global and Concur (Classic) Pay applications are a portion of the expense and invoice component of Concur's product offerings. The offerings reimburse employees and pay credit card invoices. **Travel:** ▪ Concur facilitates the purchasing of travel on behalf of their customers and transmits the information to Global Distribution System (GDS) suppliers and Direct Connect Partners. ▪ Customers manage travel reservations, including purchasing, changing, and cancellations of reservations through the Concur Travel application. Customers can store credit cards on file, where Concur stores: PAN, cardholder name, and expiration date. ▪ Some travel reservations, dependent on the Direct Connect Partner, require the card verification code (CVV) for the processing of transactions. Concur requests that information at the time of the transaction from the cardholder, and only holds that information in non-volatile memory, and sends to the Direct Connect Partner. Card verification codes are never stored. ▪ Customers can enter new credit cards at the time of travel booking if they do not want to use the card on file. ▪ Data is transmitted over HTTPS TLS 1.2 connections, both inbound from the customer and outbound to GDS and Direct Connect Partners. Some GDS suppliers utilize private connections over IPsec VPN tunnels secured with strong encryption. ▪ Airplus data flows included the use of SFTP connections where files were built in memory and sent over to Airplus. Files were encrypted with Concur's 4096 PGP key prior to sending over the secured SFTP channel.

Expense:

- Credit Card Import (Corporate Card): For the Expense portion of the application, Credit Card Issuers and Clearinghouses provide PGP encrypted files over SFTP to Concur, for the purpose of expense management on behalf of their customers. Concur utilizes PGP encrypted files sent outbound to customers, over SFTP.
- SAE (Standard Accounting Extract): SAE files of expense data are created and transmitted to customers via SFTP encrypted with the customers PGP key and over FTPS or SFTP connections.
- Detokenizer: Allowed customers to utilize a token that represented a credit card to retrieve the real PAN from the expense database over HTTPS. Once the PAN was retrieved it was encrypted with the customers PGP public key and sent back to the customer over HTTPS.
- Concur Classic Pay: Concur pays the corporate card issuer on behalf of the customer. Card data IFM files are encrypted with the issuer's PGP public key and SFTP off to the customer.
- Global Pay: Expense pay sends CHD data Bambora and Western Union over HTTPS for the purpose of paying expenses on behalf of the corporate cardholder.
- Concur has functionality to pay the issuer on behalf of the cardholder where PAN is transmitted to the issuer.

Storage:

- Concur stored CHD elements including PAN, cardholder name, and expiration. The elements stored was dependent on the application and usage.
- CHD storage locations included database tables, database backup file locations on NAS, and flat file NAS locations. All NAS appliances utilized AES-256 disk encryption.
- Data within the different travel and expense databases were stored with column level AES 256-bit encryption.
- Database backups including AES 256-bit encrypted data were stored on NAS appliances with AES-256 disk encryption.
- SFTP SAE inbound files were stored temporarily on NAS appliance mounted storage locations encrypted
- Outbound SAE SFTP files were temporarily on NAS appliance mounted storage locations encrypted with the recipient's public key. Best practices were provided for key strength and rotation of these keys but the responsibility for all key management and strength were the responsibility of the recipient.

	▪ IFM Archive files were stored encrypted with PGP RSA 4096-bit asymmetric keys utilizing AES 256-bit symmetric keys. ▪ IFM Batch files were stored encrypted with PGP encryption
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):
Example: Retail outlets	*3*	*Boston, MA, USA*
Colocations EMEA	2	Amsterdam, Netherlands; Paris, France

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)
Not applicable.	Not applicable.	Not applicable.	☐ Yes ☐ No	Not applicable.
			☐ 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).*	**Processes:** Travel: Card-Not-Present transactions including PAN, expiry, CVV (dependent on partner), cardholder name; Travel bookings including new reservations, changes, and cancellations; Transmission of CHD to GDS and Direct

• *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	Connect partners; Transmission was over SFTP, FTPS, HTTPS TLS 1.2, and/or IPSec VPN Expense: Concur received expense data from multiple sources including customers, credit card issuers & clearinghouses. Payment channels were the responsibility of the provider of the data and could come from card-present and card-not-present transactions. Data was transmitted over SFTP, FTPS, HTTPS TLS 1.2, and/or IPSec VPN **Technologies:** Concur Travel and Expense Web Applications; SFTP technologies; remote technologies including VPN, RDP, SSH; firewalls; routers; switches; load balancers; web application firewalls; containers; PGP encryption; AES 256-bit encryption; HTTPS TLS 1.2 connections; IPSec VPN private connections; file integrity monitoring; proxy servers; databases; batch servers; archive servers; NAS appliances; bastion servers; Okta authentication and multi-factor; vault encryption appliances; SIEMS; anti-virus; secrets vault; active directory; domain controllers; NTP Tiered architecture including: ▪ Untrusted: Client Tier, Partners, GDS & DirectConnect, Payment Service Providers ▪ DMZ: Edge firewalls, Proxy servers, Web Tier, Edge servers for SFTP/FTPS, Container EcoSystem ▪ Mid-Tier: Expense Mid-Tier, Travel Mid-Tier ▪ Storage: NetApp NAS ▪ Infra/Tools: Security Tools, Bastion Hosts, Tools ▪ Data Tier: Databases on CTE Production DB VLANs, Exagrid backup NAS
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:**
Akamai	SaaS Web Application Firewall
Equinix	Colocation provider
Okta	SaaS authentication, authorization provider
Prosys	Data disk destruction provider
Sophos	SaaS anti-virus 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 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:	Concur Travel and Expense (CTE)

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:	☒	☐	☐	
Requirement 2:	☐	☒	☐	2.1.1: Not applicable. CTE did not have any wireless networks within or connected to their CDE. 2.6: Not applicable. CTE was not a shared hosting provider.
Requirement 3:	☒	☐	☐	
Requirement 4:	☐	☒	☐	4.1.1: Not applicable. CTE did not utilize wireless within or connected to their CDE.
Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	6.4.6: Not applicable. CTE did not have any significant changes.
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	8.1.5: Not applicable. CTE did not allow third parties access to production. 8.5.1: Not applicable. CTE did not have access to customer premises.
Requirement 9:	☐	☒	☐	9.8.1: Not applicable. CTE did not utilized hard-copy materials with CHD. 9.9 – 9.9.3: Not applicable. CTE did not utilize POI devices within their environment.
Requirement 10:	☒	☐	☐	

Requirement 11:	☐	☒	☐	11.1.1: Not applicable. CTE did not have any authorized wireless devices.
Requirement 12:	☐	☒	☐	12.3.9: Not applicable. CTE did not allow vendors or business partners access to the production environment.
Appendix A1:	☐	☐	☒	A1.1 – A1.4: Not applicable. CTE was not a shared hosting provider.
Appendix A2:	☐	☐	☒	A2.1 – A.2.3: Not applicable. CTE did not utilize POI devices within their environment.

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:	*February 10, 2021*	
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 *February 10, 2021.*

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 *Concur Technologies, Inc.* 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: TBD 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, Inc.*

Part 3b. Service Provider Attestation

DocuSigned by:
Saju Pillai
9547BD32D2694E2...

Signature of Service Provider Executive Officer ↑	*Date:* 2/10/2021
Service Provider Executive Officer Name: **Saju Pillai**	*Title:* **Chief Technology Officer**

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

If a QSA was involved or assisted with this assessment, describe the role performed:	Independent Assessor

DocuSigned by:
Doug Kanney
E2B3593E0A364CA...

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* 2/10/2021
Duly Authorized Officer Name: Doug Kanney	*QSA Company:* Schellman & Company, LLC

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:	*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	☒	☐	Refer to part 2g for details of requirement applicability.
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	Refer to part 2g for details of requirement applicability.
3	Protect stored cardholder data	☒	☐	Refer to part 2g for details of requirement applicability.
4	Encrypt transmission of cardholder data across open, public networks	☒	☐	Refer to part 2g for details of requirement applicability.
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	Refer to part 2g for details of requirement applicability.
6	Develop and maintain secure systems and applications	☒	☐	Refer to part 2g for details of requirement applicability.
7	Restrict access to cardholder data by business need to know	☒	☐	Refer to part 2g for details of requirement applicability.
8	Identify and authenticate access to system components	☒	☐	Refer to part 2g for details of requirement applicability.
9	Restrict physical access to cardholder data	☒	☐	Refer to part 2g for details of requirement applicability.
10	Track and monitor all access to network resources and cardholder data	☒	☐	Refer to part 2g for details of requirement applicability.
11	Regularly test security systems and processes	☒	☐	Refer to part 2g for details of requirement applicability.
12	Maintain a policy that addresses information security for all personnel	☒	☐	Refer to part 2g for details of requirement applicability.
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	☒	☐	Refer to part 2g for details of requirement applicability.
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☒	☐	Refer to part 2g for details of requirement applicability.