



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:	PayPal Inc.		DBA (doing business as):	PayPal		
Contact Name:	Jason Hansen		Title:	Director – Technology and Information Security Compliance		
Telephone:	480.862.8632		E-mail:	jashansen@paypal.com		
Business Address:	2211 N 1 st St		City:	San Jose		
State/Province:	CA	Country:	USA		Zip:	95131
URL:	www.paypal.com					

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

Company Name:	K3DES, LLC				
Lead QSA Contact Name:	Howard Glavin	Title:	Executive Vice President		
Telephone:	904.631.9204	E-mail:	Howard.Glavin@k3des.com		
Business Address:	9037 Larston Street	City:	Houston		
State/Province:	TX	Country:	USA	Zip:	77055
URL:	www.k3des.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: All Services Assessed

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): Account Linking, Pay with Rewards & UPI QRC and Card issuing

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.

PayPal provides both on-line and offline payment solutions. Buyers and sellers on e-tailers, on-line businesses, and traditional off-line businesses can use PayPal's payment products to complete payment for their e-commerce transactions and in-store transactions. Customers create and fund their accounts through the Company's website/mobile applications or through links from a merchant's website. Accounts are funded using a credit card, debit card, bank accounts, checks, PayPal Credit, or funds held in their account as a PayPal balance. In addition, PayPal also issues virtual and physical (with the help of partners) PANs for merchants and consumers data flows.

PayPal processes and or gateways Card Present, Card Not Present and PIN-Debit transactions both directly (user comes directly to PayPal) and indirectly (user inputs in merchant site and is forwarded to PayPal) as well as functions as a collective Merchant for their customer base for authorization and settlement of charges to their merchant clients on their behalf. PayPal also issues card instruments that could be used at both PayPal point of sale systems and also at other point of sale locations that support the issuing brand. PayPal issued virtual tokens can also be used at both in-store and online payment use cases.

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):
<i>Example: Retail outlets</i>	3	<i>Boston, MA, USA</i>
Data Centers	7	Phoenix, AZ, USA Salt Lake City, UT, USA Las Vegas, NV, USA Chandler, AZ, USA Denver, CO, USA Bluffdale, UT, USA West Jordan, UT, USA
POP/Secondary Data Centers	18	Ashburn, VA, USA Sao Paulo, Brazil Chicago, IL, USA Los Angeles, CA, USA



		San Jose, CA, USA Hong Kong, China Shanghai, China Singapore Sydney, Australia Tokyo, Japan Amsterdam, Netherlands Dublin, Ireland Frankfurt, Germany Istanbul, Turkey London, UK Luxembourg Moscow, Russia Dallas, TX, USA
Corporate Offices – Compliance Zone	4	Dublin, Ireland Dundalk, Ireland Omaha, NE, USA Chandler, AZ, USA
Corporate Offices – Customer Service Centers	11	Berlin, Germany Chandler, AZ, USA Dublin, Ireland Dundalk, Ireland Hunt Valley, MD, USA Manila, Philippines Omaha, NE, USA Sao Paulo, Brazil Shanghai, China Chennai, India Bangalore, India

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	N/A	N/A	<input type="checkbox"/> Yes <input type="checkbox"/> 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).

PayPal stores and processes card holder data in well-defined security zones that are segmented from the remaining network environments. K3DES, LLC included the coverage of all critical systems within these security zones to include: Firewalls, Routers, Switches, Servers, Applications, Databases,



- *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*

and Workstations. K3DES, LLC also included physical security, facility security, employee compliance with policy, and all connections into and out of the CDE.

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

This report is generated for
juan@the.company



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:

American Express

Payment Processor

Bancomer

Payment Processor

Bank of America

Payment Processor

Banorte

Payment Processor

Barclays

Payment Processor

BNPP

Payment Processor

Chase Paymentech

Payment Processor

Citibank

Payment Processor

Deutsche Bank

Payment Processor

Digital River World Payments

Payment Processor

Discover Financial Services, LLC

Payment Processor

Elavon

Payment Processor

Empereon Constar

Payment Processor

First Data Resources LLC – Fiserv Solutions

Payment Processor

Fidelity Information Services

Payment Processor

Global Payments

Payment Processor

Merchant E Solutions

Payment Processor

Moneris

Payment Processor

Omnipay (a division of First Data International)

Payment Processor

TSYS Vital

Payment Processor

Vantiv

Payment Processor



Wells Fargo Bank	Payment Processor
Wells Fargo Merchant Services	Payment Processor
Westpac	Payment Processor
WorldPay UK Limited	Payment Processor
Mastercard Send (Push Payments)	Payment Processor
First Data Merchant Services	Payment Processor
Google Cloud Platform	Data Hosting Service
Mediamedics	Payment Processor
NTT Data	Payment Processor
StarFinanz	Payment Processor
STAR Network, Inc.	Payment Processor
The Bancorp, Inc.	Payment Processor
Trustly	Payment Processor
Voclink	Payment Processor
VTB24	Payment Processor
Visa Direct (OCT)	Payment Processor
Visa Direct Connect (DEX)	Payment Processor
Mastercard Direct Connect (ISO)	Payment Processor
Accesstage	Payment Processor
Worldline	Payment Processor
Sitel Dessau	Customer Service Center
Synchrony Bank: Card Production Certified	Credit Card Issuer
Aligned Energy	Data Center Services
BCS FM Solutions	Data Center Services
Databank Holdings Ltd.	Data Center Services
Digital Realty Trust	Data Center Services
Equinix Berkshire	Data Center Services
Microsoft Azure	Cloud Data Hosting Service
EFTPOS	Payment Processor
T-5 Data Centers	Data Center 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:	<p>Card Present: Merchant - PayPal Here SDK and PayPal Here mobile App</p> <p>Card Not Present: Merchant</p> <ul style="list-style-type: none"> • PayPal Checkout • PayPal for Marketplaces • Subscriptions • Invoicing • PayPal Plus • Billing Agreement • Billing Plans • Payments API • Vault API • PayPal Payments Standard • PayPal Payments Pro/Payflow Gateway • Website Payments Pro • PayPal Payments Pro • Account Linking • Pay with Rewards • UPI QRC and Card issuing <p>Card Present: Consumer - PayPal Cash Card</p> <p>Card Not Present: Consumer</p> <ul style="list-style-type: none"> • PayPal Consumer Mobile Application (Android, iOS) • PayPal Consumer Web Application • PayPal P2P Partner Integrations (Example: MS-Outlook)
	Details of Requirements Assessed



PCI DSS Requirement	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:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2.1.1 - Not Applicable - No wireless in the environment; 2.6 – Not a shared hosting provider
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3.4.1 – Disk encryption not in use; 3.6.6 – No manual clear-text cryptographic key-management operations are used
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	4.1.1 - Not Applicable - No wireless in the environment; 4.2 – End-user technologies not used to send CHD
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 6:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	6.4.6 – No significant changes occurred
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 8:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	8.5.1 – PayPal has no remote access to customers
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	9.5.1 - No back up media in off-site locations; 9.6.2 - No media sent off site; 9.9.x – No Card Interaction Devices
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	11.2.3 – No significant changes occurred
Requirement 12:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not a shared hosting provider
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	No SSL or Early TLS in use



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:	15 October 2022	
Have compensating controls been used to meet any requirement in the ROC?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the ROC identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Were any requirements not tested?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No

This report is generated for
juan@the.company



Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated **15 October 2022**.

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**):

<input checked="" type="checkbox"/>	<p>Compliant: All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby <i>PayPal Inc</i> has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p>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 (<i>Service Provider Company Name</i>) has not demonstrated full compliance with the PCI DSS.</p> <p>Target Date for Compliance:</p> <p>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. <i>Check with the payment brand(s) before completing Part 4.</i></p>						
<input type="checkbox"/>	<p>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.</p> <p><i>If checked, complete the following:</i></p> <table border="1"> <thead> <tr> <th>Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met				
Affected Requirement	Details of how legal constraint prevents requirement being met						

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to the <i>PCI DSS Requirements and Security Assessment Procedures</i> , Version 3.2.1, and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
<input type="checkbox"/>	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	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)

<input checked="" type="checkbox"/>	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.
<input checked="" type="checkbox"/>	ASV scans are being completed by the PCI SSC Approved Scanning Vendor <i>Temable.io</i>

Part 3b. Service Provider Attestation

DocuSigned by: <i>Assaf Keren</i> FADA302AF1C94CF...	
Signature of Service Provider Executive Officer ↑	Date: 15 October 2022
Service Provider Executive Officer Name: Assaf Keren	VP, Enterprise Cyber Security - CISO

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

If a QSA was involved or assisted with this assessment, describe the role performed:	Full assessment and RoC
DocuSigned by: <i>Howard Glavin</i> 7428BA862AE649B...	
Signature of Duty Authorized Officer of QSA Company ↑	Date: 15 October 2022
Duty Authorized Officer Name: Howard Glavin	QSA Company: K3DES, 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:	<p>A.Shah - Technology and InfoSec Compliance Lead – Documentation/Evidence review, Liaison and Facilitator</p> <p>S.Swaminathan – Coordination of reviews, meetings, evidence, and documentation.</p> <p>V.Malhotra – Coordination of reviews, meetings, evidence, and documentation.</p> <p>S.Singh - Coordination of reviews, meetings, evidence, and documentation.</p>
---	---

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

