Payment Card Industry (PCI) Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

A QSA led assessment of compliance validation according to the Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures version 3.2.1.

Level 1 Service Provider Validation: According to the service provider validation requirements defined by the payment brands (including American Express, Discover, JCB, Mastercard, UnionPay and Visa) in PCI industry, the annual onsite review by QSA for level 1 service provider could be compulsory.

CDNetworks Co., Ltd.

Report Date: August 21, 2023
Initial Compliance Date: August 9, 2021
Report Number: C953-02-2023-B

Document Changes

Date	Version	Description
September 2022	V3.2.1 Revision 2	Updated to reflect the inclusion of UnionPay as a Participating Payment Brand.

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:	CDNetworks Co., Ltd. (Branded as "CDNetworks")		DBA (doing business as):	N/A	
Contact Name:	Doyle Deng		Title:	Senior Information Security and Privacy Compliance Specialist	
Telephone:	+86 18596835679		E-mail:	doyle.deng@cdnetworks.com	
Business Address:	7F, 34, Mareunnae-ro, Jung-gu, Seoul, 04555 Rep. of Korea		City:	Seoul	
State/Province:	-	Country:	P.R. Korea	-	Country:
URL:	https://www.cdnetworks.co.kr/				

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

Company Name:	atsec (Beijing) Information Technology Co., Ltd				
Lead QSA Contact Name:	Xiangdong Gao		Title:	QSA, Principal Consultant	
Telephone:	+86 10 5305 6679 - 605		E-mail:	xiangdong@atsec.com	
Business Address:	3/F, Block C, Bld.1, Boya C-Center, Life Science Park, Changping District, Beijing, P.R. China		City:	Beijing	
State/Province:	-	Country:	P.R. China	Zip:	102206
URL:	https://www.atsec.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:	Secured Internet Content Delivery Network Acceleration service

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		
☐ 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): Secured Internet Content Delivery Network Acceleration service		

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:	Internet Content Delivery Network Acceleration service	
Type of service(s) not assessed:		

Hosting Provider:	Managed Services (specify):	Payment Processing:
☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	☐ 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:	This business is another type of CDN acceleration service, which does not provide secure data transmission. Because the data transmission is not encrypted in this business, it is not recommended for the payment industry customer to choose this non-protected CDN acceleration service. And based on business decision from CDNetworks, this business is out of the scope of this PCI DSS assessment.

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	CDNetworks provides online business services, like Internet Content Delivery Network Acceleration (CDN), Secured Internet Content Delivery Network Acceleration service, cloud distribution service and High-speed Data Transmission (HDT) service. This assessment only focuses on Secured Internet Content Delivery Network Acceleration service. As a content distribution and acceleration service provider, its Content Delivery Network (CDN) nodes connect to the customers' servers and cache servers' site contents. When an Internet user access to the customers' site, CDNetworks 's nearest CDN node then responses to the request and provides Internet users with access acceleration service. CDNetworks's customers include e-business merchants, payment service providers, banks, etc. During the data transmission, CDNetworks provides these entities with strong HTTPS cryptographic transmission tunnels based on the certificates provided by its customers. Cardholder data (PANs, Cardholder name and Expiry date) and sensitive authentication data (CVV2, CVC2, CAV, CID and CVN2) are transmitted via network appliances and application servers. Neither cardholder data nor sensitive authentication data are stored in the cardholder data environment.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Internet Content Delivery Network Acceleration for non-encryption data transmission is located in separate physical CDN system components and have no connection to the secured Internet Content Delivery Network Acceleration, and thus there is no other business has the ability to impact the security of cardholder data.

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*
Office Network	1	Office network is located at No. B19, Plan III of Software Park, Jimei District, Xiamen City, Fujian Province, P.R. China
Branch network	49	Node "AH-huainan13-YD" is located at No. 1 Building, China Mobile Huainan Datacenter, High-

		tech Development Zone, Huainan City, An'hui Province, P.R. China
		Node "BJ4-YD" is located at Floor 5th, No.1 Gongti North Road, Chaoyang District, Beijing, P.R. China
		Node "BJ-zhaowei3-DX" is located at Floor 3rd, Entrance 2nd, No. 1 Building, Area D Zhaowei Industry Park, No. 14 Jiuxianqiao Road, Chaoyang District, Beijing City, P.R. China
		Node "Germany_FRA2" is located at c/o Interxion Deliveries, Hanauer Landstrasse 302, D-60314 Frankfurt am Main, GermanyFRA11, Room 432, R51B02-R51B05
		Node "FJ-quanzhou-YD" is located at Floor 2nd, Quanzhou Mobile Telecommunication Datacenter, No.567, Anji Road, Fengze District, Quanzhou City, Fujian Province, P.R. China
		Node "GD-guangzhou10-YD" is located at Room 403, Plaza C, No. 1, Ruiqi Science and Technology Park, Nanxiang 2nd Road, Huangpu District, Huangzhou City, Guangdong Province, P.R. China
		Node "GD-jiangmen5-DX" is located at Floor 15, China Telecom Building, No.2 Huanshiyi Road, Pengjiang District, Jiangmen City, Guangdong Province, P.R. China
		Node "GZ-guian-DX" is located at China Telecom cloud computing Guizhou information park, Qianzhong Avenue, Machang Town, Pingba District, Anshun City, Guizhou Province, P.R. China
		Node "HB-baoding5-WT" is located at Zhuzhou China Unicom Building, No.169 Fanyang middle Road, Zhuzhou City, Hebei Province, P.R. China
		Node "HB-handan-WT" is located at China Unicom information Building, Renmin Road, Handan City, Hebei Province, P.R. China
		Node "HA-zhumadian-WT" is located at Floor 6th, China Unicom IDC center, Tuanjie Road, Yicheng District, Zhumadian City, Henan Province, P.R. China
		Node "HLJ-suihua-WT" is located at No. 84 North 2nd East Road, China Unicom Company, Suihua City, Heilongjiang Province, P.R. China
		Node "HB-xiangyang-YD" is located at Mobile Telecommunication Xiangyang Cloud computing center, Dali Avenue, High-tech District, Xiangyang City, Hebei Province, P.R. China
		Node "HN-yy3-WT" is located at Floor 2nd, Military-civilian Integration Industrial Park, 6906 Yungang Road, Lingang New District, Chenglingji, Yueyang City, HunanProvince, P.R. China
		Node "JL-siping-WT" is located at Floor 18th, China Unicom Building, No. 455 Nanyoudian Streect, Tiexi Distirct, Siping City, Jilin Province, P.R. China

		Node "JL-changchun4-YD" is located at Floor 2nd, No. 1566 Jinhu Road, High-tech Zone, Changchun City, Jilin Province, P.R. China
		Node "JL-changchun4-YD" is located at Floor 4th, Mobile Telecommunication server room, Suiyuan Road, Lishui District, Nanjing City, Jiangsu Province, P.R. China
		Node "JS-yangzhouxiazai8-DX" is located at Floor 2nd, Yangzhou Super cloud computing center, Building 2nd, Import and Export Processing Zone, No.9 Jiangnan Road, Yangzhou City, Jiangsu Province, P.R. China
		Node "JS-zhenjiang2-YD" is located at Floor 3rd, Dantu Communication Center, No.201 Guyang Avenue, Dantu District, Zhenjiang City, Jiangsu Province, P.R. China
		Node "JX-jingdezhen2-DX" is located at IDC Room, Floor 8th, No. 3, Zhushan West Road, Changjiang District, Jingdezhen City, Jiangxi Province Jiangxi Province, P.R. China
		Node "JX-yichun-WT" is located at No.40 Yiyang Avenue, Yuanzhou District, Yichuan City, Jiangxi Province, P.R. China
		Node "USA-DEN1" is located at 910 15th St., Suite 740, Denver, CO 80202
		Node "USA_SEA2" is located at Tierpoint 100 4th Avenue N. Seattle, WA 98109
		Node "NX-yinchuan-YD" is located at Room 214, Floor 1st, No.2 Building Ningxia Mobile Telecommuincation Xixia Product Center, No. 196 JIngtiandong Road, Xixia District, Yinchuan City, Ningxia Province, P.R. China
		Node "JP_TYO4" is located at 2-1-7 Higashi-shinagawa, Tokyo, 140-0002 Japan
		Node "SD-qingdaoxiazai-DX" is located at Blue Bay Enterprise Park, Jinhui Road, Chengyang District, Qingdao City, Shandong Province, P.R. China
		Node "SD-zibo-WT" is located at IDC Room, Floor 2nd, No. 1, Communist Youth League West Road, Zhangdian District, Zibo City, Shangdong Province, P.R. China
		Node "SX-xianyang3-DX" is located at Room 802, Floor 8th, China Telecom Building, No. 1 Leyu North Road, Weicheng District, Xianyang City, Shaanxi Province
		Node "SH-jingan-YD" is located at Shuchuan Room, Floor 4, No.1001 Zhongshanbei Road, Jing'an District, Shanghai City, P.R. China
		Node "SC-chengdu5-DX" is located at Floor 2nd, No.2007, Section 3, Guanghua Avenue, Wenjiang District, Chengdu City, Sichuan Province, P.R. China

		Node "SC-meishan2-WT" is located at Floor 1st, No. 1, Unicom Road, Kegong Park, Dongpo District, Meishan City, Sichuan Province, P.R. China
		Node "TJ-DX" is located at IDC Room, 2nd Floor, China Telecom, No. 18, Guangming Road, Wuqing Economic Development Zone, Tianjin City, P.R. China
		Node "TJ-konggang-WT" is located at Tianjin Unicom main Building, Xiqi Street, Airport Economic Zone, Binhai New District, Tianjin City, P.R. China
		Node "TJ-tianjin6-YD" is located at Room 203, Floor 2nd, Zhongbei Industrial Park, Qufu Sheng Road, Xiqing District,Tianjin City, P.R. China
		Node "Singapore-Sin1" is located at 26A Ayer Rajah Crescent, Singapore 139963.
		Node "Singapore-Sin5" is located at 2 Tai Seng Avenue, Singapore 534408.
		Node "SG_SIN6" is located at 2 Tai Seng Avenue, Singapore 534408.
		Node "England_LON4" is located at Coriander Avenue London E14 2AA UK.
		Node "YN-chuxiong5-DX" is located at Floor 8th, China Telecom Production Building, No. 366 Yong 'an Road, Development Distirct, Chuxiong City, Yunnan Province, P.R. China
		Node "YN-kunming6-YD" is located at China Mobile Yunnan Chenggong Datacenter, Zhihui Road, Wujiaying Street, Chenggong District, Kunming City, Yunnan Province, P.R. China
		Node "ZJ-shaoxing2-YD" is located at Floor 4th, NO. 98 Pingjiang Road, Yuecheng District, Shaoxing City, Zhejiang Province, P.R. China
		Node "ZJ-wenzhou10-DX" is located at Floor 4th, No. 788, Mingzhu Road, Longwan District, Wenzhou City, Zhejiang Province, P.R. China
		Node "ZJ-wenzhou5-DX" is located at No. 2 Fuchunjiang Road, Economy and Technology Development Zone, Wenzhou City, Zhejiang Province, P.R. China
		Node "ZJ-zhoushanxiazai-WT" is located at Floor 5th, No. 268 Linchenghaiyu Road, Dinghai District, Zhoushan City, Zhejiang Province, P.R. China
		Node "CQ-shuitu-DX" is located at China Telecom Cloud Computing Chongqing Base, Yunfu Road, Shushui Town, Beibei District, Chongqing City, P.R. China
		Node "CQ-YD5" is located at Room 407, China Mobile Chongqing (Shuitu) Data Center, No. 775 Taihe Road, Beibei District, Chongqing, P.R. China
		Node "ZJ-ningbo-YD" is located at Building D01, No. 1208 Binhai Sixth Road, Hangzhou Bay New District, Ningbo City, Zhejiang Province, P.R. China

		Node "Sejong (ONSE) IDC" is located at 85 Yonggu-daero 277 1beon-gil, Suji-gu, Yongin-si, Gyeonggi-do, Republic of Korea.
		Node "Lotte IDC" is located at 17-9 Mabuk-ro 240beon-gil, Giheung-gu, Yongin-si, Gyeonggi-do, Republic of Korea.

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)
Configuration Management Platform	Version v1.150.0	CDNetworks	☐ 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 system components of the cardholder data environment are located at CDNetworks global CDN node datacenters, which mainly connect to end users and customers over Internet. The location of CDN node datacenters is listed in part 2c. Office network for administration has connections into the CDE, which is located at Xiamen office. The critical system components involved in the cardholder data environment include load balance servers and HTTPS acceleration servers in CDN node. and secure management servers, such as VPN server, Bastion server, etc.
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:**
Not applicable. Because CDNetworks has no connection to third-party service providers.	

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:	Secured Internet Content Delivery Network Acceleration service			
	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:	☐	☒	☐	Requirement 1.2.2 was marked as not applicable. Because router devices are not implemented in the cardholder data environment. Requirement 1.2.3 was marked as not applicable. Because wireless technologies are not enabled in the CDE and out-of-scope wireless networks have no connection to the CDE. Requirement 1.3.6 was marked as not applicable. Because cardholder data are not stored in any server of the cardholder data environment.
Requirement 2:	☐	☒	☐	Requirement 2.1.1 was marked as not applicable. Because wireless technologies are not enabled in the CDE and out-of-scope wireless networks have no connection to the CDE. Requirement 2.2.3 was marked as not applicable. Because insecure protocols services and daemons are not enabled in the cardholder data environment. Requirement 2.6 was marked as not applicable. Because CDNetworks is not shared hosting provider and no any other shared hosting providers are involved in this PCI DSS assessment.
Requirement 3:	☐	☒	☐	Requirement 3.1 was marked as not applicable. Because cardholder data and sensitive authentication data are not stored in the cardholder data environment. Requirement 3.3 was marked as not applicable. Because neither mask PANs nor full PANs are visible to internal personnel.

				Requirements 3.4 and 3.4.1 were marked as not applicable. Because cardholder data are not stored in the cardholder data environment.
				Requirements 3.5, 3.5.1, 3.5.2, 3.5.3, 3.5.4, 3.6, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7, and 3.6.8 were marked as not applicable. Because cardholder data are not stored in the cardholder data environment and thus encryption keys are not used to protect cardholder data.
Requirement 4:	☐	☒	☐	Requirement 4.1.1 was marked as not applicable. Because wireless technologies are not enabled in the CDE and out-of-scope wireless networks have no connection to the CDE.
				Requirement 4.2 was marked as not applicable. Because PANs are not transmitted via end-user messaging technologies.
Requirement 5:	☒	☐	☐	All requirements in this section were marked as applicable.
Requirement 6:	☐	☒	☐	Requirement 6.4.3 was marked as not applicable. Because PANs are not required for testing procedure.
				Requirement 6.4.6 was marked as not applicable. Because significant change was not occurred within past 12 months.
Requirement 7:	☒	☐	☐	All requirements in this section were marked as applicable.
Requirement 8:	☐	☒	☐	Requirement 8.1.5 was marked as not applicable. Because vendor accounts are not enabled in the cardholder data environment.
				Requirement 8.5.1 was marked as not applicable. Because CDNetworks has not remote access to its customer premises.
				Requirement 8.7 was marked as not applicable. Because cardholder data are not stored in database servers.
Requirement 9:	☐	☒	☐	Requirements 9.5, 9.5.1, 9.6, 9.6.1, 9.6.2, 9.6.3, 9.7, 9.7.1, 9.8, 9.8.1, and 9.8.2 were marked as not applicable. Because cardholder data is not stored in CDE, and no media is involved for the storage of cardholder data.
				Requirements 9.9, 9.9.1, 9.9.2, and 9.9.3 were marked as not applicable. Because card-present services are not supported in the cardholder data environment.
Requirement 10:	☐	☒	☐	Requirement 10.2.1 was marked as not applicable. Because there was not cardholder data stored in the CDE thus no user could access to cardholder data.
Requirement 11:	☐	☒	☐	Requirement 11.1.1 was marked as not applicable. Because wireless access points are not enabled in the cardholder data environment.

Requirement 12:	☐	☒	☐	Requirement 12.8.5 was marked as not applicable. Because no PCI DSS requirements are managed by external entities.
Appendix A1:	☐	☐	☒	All requirements were marked as not applicable. Because CDNetworks is not shared hosting provider and no any other shared hosting providers are involved in this PCI DSS assessment.
Appendix A2:	☐	☐	☒	All requirements were marked as not applicable. Because POS POI terminals are not enabled in the cardholder data 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:	August 21, 2023
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 *August 21, 2023*.

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 *CDNetworks Co., Ltd.* 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 *CDNetworks Co., Ltd.* 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 *atsec (Beijing) Information Technology Co., Ltd*

Part 3b. Service Provider Attestation

Doyle Deng

Signature of Service Provider Executive Officer ↑	Date: August 18, 2023
Service Provider Executive Officer Name: Doyle Deng	*Title: Senior Information Security and Privacy Compliance Specialist*

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

If a QSA was involved or assisted with this assessment, describe the role performed:	QSA assessment and evidence validation.

Xiangdong Gao

Signature of Duly Authorized Officer of QSA Company ↑	Date: August 18, 2023
Duly Authorized Officer Name: Xiangdong Gao (高向东)	*QSA Company: atsec (Beijing) Information Technology Co., 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:	Not applicable. Because ISA is not involved in this PCI DSS assessment.

---

[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 Require ment	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	☒	☐	