Payment Card Industry

Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0.1

Publication Date: August 2024

PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: PayGuard Solutions Ltd

Date of Report as noted in the Report on Compliance: 2026-10-16

Date Assessment Ended: 2026-09-30

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance (AOC) must be completed as a declaration of the results of the service provider's assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures (*"Assessment"). Complete all sections. The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which this AOC will be submitted for reporting and submission procedures.

This AOC reflects the results documented in an associated Report on Compliance (ROC). Associated ROC sections are noted in each AOC Part/Section below.

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Report on Compliance Template.

Part 1. Contact Information

Part 1a. Assessed Entity (ROC Section 1.1)	
Company name:	PayGuard Solutions Ltd
DBA (doing business as):	PayGuard Solutions Ltd
Company mailing address:	71-75 Shelton Street, Covent Garden, London, United Kingdom, WC2H 9JQ
Company main website:	https://payguard.co/
Company contact name:	Mr. Ioan Alexandru Din
Company contact title:	Head of Product
Contact phone number:	0747 8384795
Contact e-mail address:	alex@payguard.co

Part 1b. Assessor (ROC Section 1.1)	
Provide the following information for all assessors involved in the Assessment. If there was no assessor for a given assessor type, enter Not Applicable.	
PCI SSC Internal Security Assessor(s)	
ISA name(s):	Not Applicable
Qualified Security Assessor	
Company name:	1 Cyber Valley
Company mailing address:	128 City Road, London, United Kingdom, EC1V 2NX
Company website:	www.onecybervalley.com
Lead Assessor name:	Ms. Shagun Agarwal
Assessor phone number:	+91 8104639371
Assessor e-mail address:	Shagun@onecybervalley.com
Assessor certificate number:	PCI QSA- 206-350

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the Assessment (select all that apply):

Name of service(s) assessed:	E-Commerce and MOTO services through Payguard Application	
Type of service(s) assessed:		
Hosting Provider: ☒ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web-hosting services ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Multi-Tenant Service Provider ☐ Other Hosting (specify):	**Managed Services:** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☐ POI / 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 these categories do not apply to the assessed service, complete "Others." If it is not clear whether a category could apply to the assessed service, consult with the entity(ies) to which this AOC will be submitted.*

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Part 2. Executive Summary *(continued)*

Part 2a. Scope Verification *(continued)*

Services that are provided by the service provider but were NOT INCLUDED in the scope of the Assessment (select all that apply):

Name of service(s) not assessed:	Not Applicable

Type of service(s) not assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POI / 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-hosting services		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service 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):		

Provide a brief explanation why any checked services were not included in the Assessment:	Not Applicable

Part 2b. Description of Role with Payment Cards (ROC Sections 2.1 and 3.1)

Describe how the business stores, processes, and/or transmits account data.	PayGuard provides both Mail Order / Telephone Order (MOTO) and E-commerce payment channels that facilitate secure payment transactions for its customers. Mail Order / Telephone Order (MOTO), DTMF via telephony: PayGuard accepts MOTO payments over the telephone. The cardholder enters their card details on the telephone keypad, so the agent does not see or hear them. The DTMF tones are transmitted over a secure SIP trunk and terminate in the Telephony VPC. The Telephony servers collect the digits and pass them by API to the Pay Guard application in the Payments

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

	VPC. PayGuard transmits the data to the payment service provider (PSP) over HTTPS using TLS 1.2 or higher. Account data is processed in memory only, and is not stored. E-commerce via payment link: An agent generates a unique HTTPS payment link and sends it to the customer by SMS or email. The link opens a PayGuard-hosted web form, where the customer enters their card details directly. The form is protected with HTTPS using TLS 1.2 or higher. On submission, the data is sent to the PSP for authorisation. Post-authorisation for Ecommerce & MOTO: The PSP tokenises the PAN and CVV2 and returns only an authorisation code and a truncated PAN (first six and last four digits) to PayGuard. PayGuard does not store full PAN or sensitive authentication data (SAD) at any stage. Account data is encrypted in transit.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	PayGuard operates a Telephony VPC and a Payments VPC that process and transmit cardholder data (CHD) for its MOTO (DTMF) and e-commerce (payment link) channels. Connections between these environments, and between PayGuard and the payment service provider (PSP), are encrypted using TLS 1.2 or higher to protect the confidentiality and integrity of CHD in transit. For the e-commerce channel, PayGuard hosts the web form where the customer enters their card details. The form and its hosting infrastructure transmit CHD over HTTPS using TLS 1.2 or higher, from the customer's browser to PayGuard's systems and onward to the PSP. PayGuard does not store CHD or sensitive authentication data. However, because it hosts and manages the payment web form and the supporting infrastructure, the security of these systems directly affects the security of CHD during transmission.
Describe system components that could impact the security of account data.	Telephony VPC and Payments VPC: Process and transmit CHD. The transmission paths between them, and onward to the PSP, require protection of CHD in transit. Web form and hosting infrastructure: Transmit CHD over HTTPS using TLS 1.2 or higher, encrypting data in transit between the customer's browser, PayGuard and the PSP.

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Part 2. Executive Summary *(continued)*

Part 2c. Description of Payment Card 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 POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.* • *System components that could impact the security of account data.*	PayGuards infrastructure is hosted on AWS in a single account and is divided into three VPCs. Two of the VPCs, the Telephony VPC and the Payments VPC, contain the servers that make up the cardholder data environment (CDE). The third VPC is used internally for development and testing. Security groups are configured on each resource in the network and act as virtual firewalls, controlling inbound and outbound traffic. Application load balancers sit in front of the web servers as the ingress points and route traffic to the appropriate destinations within the network. AWS WAF and AWS Shield are attached to the load balancers and, together with antivirus, monitoring and alerting systems, help protect the infrastructure from potential attacks. Logging of system, user and process activity is implemented on all servers and systems in the CDE. Events are forwarded to centrally secured systems that provide event correlation and alerting. File integrity monitoring (FIM) is also performed on all servers and systems in the CDE.
Indicate whether the environment includes segmentation to reduce the scope of the Assessment. (Refer to the "Segmentation" section of PCI DSS for guidance on segmentation)	☐ Yes ☒ No

Part 2d. In-Scope Locations/Facilities (ROC Section 4.6)

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this Assessment.

Facility Type	Total Number of Locations (How many locations of this type are in scope)	Location(s) of Facility (city, country)
Example: Data centers	*3*	*Boston, MA, USA*
Corporate Office	1	London, United Kingdom
AWS Cloud Datacenter	3	eu-west-2a, 2b and 2c, London, United Kingdom

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Part 2. Executive Summary *(continued)*

Part 2e. PCI SSC Validated Products and Solutions (ROC Section 3.3)

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions*?

☐ Yes ☒ No

Provide the following information regarding each item the entity uses from PCI SSC's Lists of Validated Products and Solutions:

Name of PCI SSC validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which Product or Solution Was Validated	PCI SSC Listing Reference Number	Expiry Date of Listing
Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD

* For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components, appearing on the PCI SSC website (www.pcisecuritystandards.org) (for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions), and Mobile Payments on COTS (MPoC) products.

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Part 2. Executive Summary *(continued)*

Part 2f. Third-Party Service Providers (ROC Section 4.4)

For the services being validated, does the entity have relationships with one or more third-party service providers that:

• Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs, and off-site storage))	☒ Yes ☐ No
• Manage system components included in the entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers)	☒ Yes ☐ No
• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	☒ Yes ☐ No

If Yes:

Name of Service Provider:	Description of Services Provided:
Amazon Web Services	Cloud Hosting Provider
Access Paysuite (Pay360)	Transaction processing
Cardstream Paya CardServices	Transaction processing Transaction processing
FIS WorldPay	Transaction processing
Stripe	Transaction processing
Opayo (Elavon)	Transaction processing
Global Payments	Transaction processing
Verifone	Transaction processing
PXP Financial	Transaction processing
Barclays	Transaction processing

Note: *Requirement 12.8 applies to all entities in this list.*

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment (ROC Section 1.8.1)

Indicate below all responses provided within each principal PCI DSS requirement.

For all requirements identified as either "Not Applicable" or "Not Tested," complete the "Justification for Approach" table below.

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: E-Commerce and MOTO services through Payguard Application

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If a Compensating Control(s) Was Used
	In Place	Not Applicable	Not Tested	Not in Place	
Requirement 1:	☒	☒	☐	☐	☐
Requirement 2:	☒	☒	☐	☐	☐
Requirement 3:	☒	☒	☐	☐	☐
Requirement 4:	☒	☒	☐	☐	☐
Requirement 5:	☒	☒	☐	☐	☐
Requirement 6:	☒	☒	☐	☐	☐
Requirement 7:	☒	☐	☐	☐	☐
Requirement 8:	☒	☒	☐	☐	☐
Requirement 9:	☒	☒	☐	☐	☐
Requirement 10:	☒	☒	☐	☐	☐
Requirement 11:	☒	☒	☐	☐	☐
Requirement 12:	☒	☒	☐	☐	☐
Appendix A1:	☐	☒	☐	☐	☐
Appendix A2:	☐	☒	☐	☐	☐

Justification for Approach

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	1.2.6- No insecure services and ports are allowed. 1.3.3- No wireless network in scope. 2.2.5- There are no insecure services running in PayGuard network. 2.3.1, 2.3.2- No wireless environment in scope. 3.3.1.1- There is no track data used in PayGuard. 3.3.1.3- There is no PIN data used in PayGuard environment. 3.3.2 - PayGuard does not store any SAD prior to authorization. 3.3.3- PayGuard is not an issuer and does not support issuing services. 3.4.2 - No remote access technologies has been implemented. 3.5.1.1- PAN is truncated instead of being encrypted. 3.5.1.2, 3.5.1.3- There is no disk level encryption methodology used in PayGuard environment. 3.6.1.3- There is no cleartext cryptographic key components to access. 3.7.6- There are no cleartext cryptographic key management operations in scope. 3.7.9- PayGuard does not share cryptographic keys with its customers. 4.2.1.2- There are no wireless networks transmitting PAN or connected to the CDE. 4.2.2- There are no end-user messaging technologies used to send PAN. 5.2.3, 5.2.3.1- There are no system components that are not at risk for malware. 5.3.3- There are no removable electronic media in PayGuard scoped environment. 6.4.1 - This requirement is superseded by Requirement 6.4.2. 6.5.2- No significant changes done in last 12 months 8.2.2- There are no group or shared accounts in PayGuard. 8.2.3- PayGuard does not have access to customer premises. 8.2.7- There is no remote access provided to third parties by PayGuard. 8.3.10 - This requirement is superseded by Requirement 8.3.10.1 8.3.10.1- PayGuard does not provide user access to their customers. 8.6.1, 8.6.2- PayGuard does not use interactive login procedure to access system and application components. 9.4, 9.4.1.1, 9.4.1.2, 9.4.2, 9.4.3, 9.4.4, 9.4.6- There is no physical media in scope 9.4.5, 9.4.5.1, 9.4.7- There is no electronic media in scope. 9.5.1, 9.5.1.1, 9.5.1.2, 9.5.1.2.1, 9.5.1.3- There are no POI devices in scope.

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

	10.7.1 - This requirement is superseded by Requirement 10.7.2. 11.2.1, 11.2.2- There are no wireless access points. 11.3.1.3, 11.3.2.1 - No significant changes made in last 12 months. 11.4.5, 11.4.6 - Segmentation is not used in PayGuard scope. 11.4.7- PayGuard is not a Multi-tenant service provider. 12.3.2- No requirements are met with customized approach. 12.5.3- No significant changes made in last 12 months. Appendix A1: PayGuard does not provide multi-tenancy services. Appendix A2: PayGuard does not manage POS devices.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	Not Applicable

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Section 2 Report on Compliance

(**ROC Sections 1.2 and 1.3**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*	2026-08-10
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	2026-09-30
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No
Were any testing activities performed remotely?	☒ Yes ☐ No

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated *(Date of Report as noted in the ROC 2026-10-16)*.

Indicate below whether a full or partial PCI DSS assessment was completed:

☒ **Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.

☐ **Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the ROC noted above, each signatory identified in any of Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document *(select one)**:***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT** rating; thereby *(*PayGuard Solutions Ltd) has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby *(Service Provider Company Name)* has not demonstrated compliance with PCI DSS requirements. **Target Date** for Compliance: *YYYY-MM-DD* An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.
☐	**Compliant but with Legal exception:** One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Service Provider Company Name)* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction. This option requires additional review from the entity to which this AOC will be submitted. *If selected, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement from being met

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Part 3. PCI DSS Validation *(continued)*

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:
(Select all that apply)

☒	The ROC was completed according to *PCI DSS*, Version 4.0.1 and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
☒	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

Ioan Alexandru Din (Oct 16, 2026 18:00:55 GMT+3)

Signature of Service Provider Executive Officer ↗	Date: 2026-10-16
Service Provider Executive Officer Name: Mr. Ioan Alexandru Din	Title: Head of Product

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this Assessment, indicate the role performed:	☒ QSA performed testing procedures.
	☐ QSA provided other assistance. If selected, describe all role(s) performed:

Shagun Agarwal

Shagun Agarwal (Oct 16, 2026 20:31:48 GMT+5.5)

Signature of Lead QSA ↗	Date: 2026-10-16
Lead QSA Name: Ms. Shagun Agarwal	

Signature of Duly Authorized Officer of QSA Company ↗	Date: 2026-10-16
Duly Authorized Officer Name: Mr. Parminder Lall	QSA Company: 1 Cyber Valley Limited

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:	☐ ISA(s) performed testing procedures.
	☐ ISA(s) provided other assistance. If selected, describe all role(s) performed:

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has Non-Compliant results noted in Section 3.

If asked to complete this section, select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement below. For any "No" responses, include the date the entity expects to be compliant with the requirement and provide a brief description of the actions being taken to meet the requirement.

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 network security controls	☐	☐	
2	Apply secure configurations to all system components	☐	☐	
3	Protect stored account data	☐	☐	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	☐	☐	
5	Protect all systems and networks from malicious software	☐	☐	
6	Develop and maintain secure systems and software	☐	☐	
7	Restrict access to system components and cardholder data by business need to know	☐	☐	
8	Identify users and authenticate access to system components	☐	☐	
9	Restrict physical access to cardholder data	☐	☐	
10	Log and monitor all access to system components and cardholder data	☐	☐	
11	Test security systems and networks regularly	☐	☐	
12	Support information security with organizational policies and programs	☐	☐	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	☐	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☐	☐	

Note: The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance accepting organization to ensure that this form is acceptable in their program. For more information about PCI SSC and our stakeholder community please visit: https://www.pcisecuritystandards.org/about_us/

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Fusion_Telecom_PCI-DSS-v4-0-1-ROC-AOC-Service-Providers_2026 (1)

Final Audit Report 2026-10-16

Created:	2026-10-16
By:	Parminder Lall (parminder@onecybervalley.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAn0D1iYlW7XumW1rAH94Ld5keoi_dykLb

"Fusion_Telecom_PCI-DSS-v4-0-1-ROC-AOC-Service-Providers_2026 (1)" History

Document created by Parminder Lall (parminder@onecybervalley.com)
2026-10-16 - 2:53:00 PM GMT- IP address: 94.9.141.49

Document emailed to alex@payguard.co for signature
2026-10-16 - 2:54:03 PM GMT

Email viewed by alex@payguard.co
2026-10-16 - 2:58:02 PM GMT- IP address: 62.231.94.54

Signer alex@payguard.co entered name at signing as Ioan Alexandru Din
2026-10-16 - 3:00:53 PM GMT- IP address: 62.231.94.54

Document e-signed by Ioan Alexandru Din (alex@payguard.co)
Signature Date: 2026-10-16 - 3:00:55 PM GMT - Time Source: server- IP address: 62.231.94.54 - Signature Appearance Selected: DRAW

Document emailed to shagun@onecybervalley.com for signature
2026-10-16 - 3:00:56 PM GMT

Email viewed by shagun@onecybervalley.com
2026-10-16 - 3:01:22 PM GMT- IP address: 104.47.85.62

Signer shagun@onecybervalley.com entered name at signing as Shagun Agarwal
2026-10-16 - 3:01:46 PM GMT- IP address: 122.161.78.140

Document e-signed by Shagun Agarwal (shagun@onecybervalley.com)
Signature Date: 2026-10-16 - 3:01:48 PM GMT - Time Source: server- IP address: 122.161.78.140 - Signature Appearance Selected: TYPE

Document emailed to Parminder Lall (parminder@onecybervalley.com) for signature
2026-10-16 - 3:01:50 PM GMT

Adobe Acrobat Sign

Email viewed by Parminder Lall (parminder@onecybervalley.com)

2026-10-16 - 3:02:06 PM GMT- IP address: 94.9.141.49

Document e-signed by Parminder Lall (parminder@onecybervalley.com)

Signature Date: 2026-10-16 - 3:02:24 PM GMT - Time Source: server- IP address: 94.9.141.49 - Signature Appearance Selected: IMAGE

Agreement completed.

2026-10-16 - 3:02:24 PM GMT

Adobe Acrobat Sign