Docusign Envelope ID: 85E51032-77A0-4DF9-AACA-96CF90E1007F



Payment Card Industry
Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0.1

Publication Date: August 2024

Docusign Envelope ID: 85E51032-77A0-4DF9-AACA-96CF90E1007F

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

Entity Name: Evervault Ltd

Date of Report as noted in the Report on Compliance: July 21, 2025

Date Assessment Ended: July 18, 2025

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

Docusign Envelope ID: 85E51032-77A0-4DF9-AACA-96CF90E1007F

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:	Evervault Ltd
DBA (doing business as):	Evervault
Company mailing address:	Exchequer Chambers, 23 Exchequer St, Dublin, D02 AC82, Ireland
Company main website:	Evervault.com
Company contact name:	John Hetherton
Company contact title:	Head of Compliance
Contact phone number:	00353 87 9628720
Contact e-mail address:	john@evervault.com

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:	Prescient Security LLC
Company mailing address:	1211 Main Street, Suite 1, Salmon, ID, 83467
Company website:	https://prescientsecurity.com/
Lead Assessor name:	Kevin Whalen
Assessor phone number:	+1 212-271-0175
Assessor e-mail address:	pci@prescientsecurity.com
Assessor certificate number:	PCI DSS QSA Certificate Number: 202-230

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

Docusign Envelope ID: 85E51032-77A0-4DF9-AACA-96CF90E1007F

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:	UI Components, API, Relay, Functions, Enclaves, 3DS, and Page Protection

Type of service(s) 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): Encryption and decryption Services, Trusted Execution Environments		

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: ☐ 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):		
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.	The following describes the services by product which Evervault provides to its customers: • UI Components: An iFrame solution managed by and served from Evervault which is embedded into customer sites facilitates reveal, collection and encryption of CHD. • Relay: A Transparent Network Encryption Proxy, which as the name suggests encrypts and decrypts data in transit. Evervault never stores the CHD, the customer does.

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

Docusign Envelope ID: 85E51032-77A0-4DF9-AACA-96CF90E1007F

	• Functions: A secure environment that can be used by customers to upload code to operate on encrypted data. Operations typically include gathering, processing and sharing CHD in a AWS Lambda based environment. • Enclaves: Enclaves is a Trusted Execution Environment, often called a confidential compute environment which again can be used by customers for processing sensitive data in a secure Enclave. Enclaves are based on the AWS Nitro Enclave technology. • Evervault API: Evervault provides a card services API which allows Evervault Customers to exchange Card Data or encrypted PANs for Network Tokens, through its connections to the Brand Networks, providing access to VISA, Mastercard, Discover and AMEX Network Tokens, Card on file services, virtual PANs retrieval, and metadata inspection on encrypted payloads which can be used for intelligent payment routing. • 3DS Service: Evervault hosts and manages a 3DS Server (3DSS) on its existing API infrastructure. The PCI DSS requirements of the systems supporting the delivery of the 3DS Server were covered in the scope of this assessment and are further subject to PCI 3DS Assessment and Attestation. • Page Protection: Evervault built Page Protection to satisfy PCI DSS requirement 6.4.3 and 11.6.1, by identifying and assessing risks associated with changes to scripts and security headers. In all the above scenarios, the customer never has direct access to the decryption keys and can only store the encrypted cardholder data. This separation of decryption key and encrypted data is beneficial to the customer as it means a breach of a customer environment cannot result in a card data breach. Similarly, Evervault never stores cardholder data, as such any breach of the key in isolation, in the absence of encrypted CHD will not result in a card data breach. **Transmission |** Evervault accepts CHD via different external channels: 1. UI Components – an authorized and authenticated iFrame service that permits clients to embed card components within an ecommerce web site payment page, to isolate the capture and transmission security responsibility to Evervault. 2. Relay – a transparent network encryption proxy service that permits clients to send encrypt and decrypt requests via API to the Evervault prior without the client needing to transmit or process the CHD. 3. API – card services API that exchanges PAN data for brand Network Tokens and for

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

Docusign Envelope ID: 85E51032-77A0-4DF9-AACA-96CF90E1007F

	processing 3DS requests, and card metadata queries. **Process |** The core Evervault product provides CHD encryption and decryption processes which involve securely encrypting and decrypting sensitive data in client segmented processing environments. The encrypted CHD is returned to the client. Evervault also provides secure processing environments, Functions (based on AWS Lambdas) and Enclaves (based on AWS Nitro Enclaves) which may be used to process cardholder data (CHD) within the secure computing environment of Evervault. **Storage** | Evervault did not store cardholder data. Evervault returns the encrypted CHD to the customers for storage, while Evervault retains and manages the encryption keys.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Evervault are responsible for the secure management of KEKs and DEKs as well as for managing the security of the processing environment which is consumed as a SaaS based model.
Describe system components that could impact the security of account data.	Evervault have several APIs which are called for the processing of CHD, these include KMS Fargate EC2 ECS RDS WAF Cloud Watch CloudTrail GuardDuty Security Hub Lambdas Nitro Enclaves GitHub Auth0 Evervault Application Evervault API These are typically based on AWS Services, which abstract much of the complexity, mundane maintenance effort involved in running a scaled global SaaS service.

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

Docusign Envelope ID: 85E51032-77A0-4DF9-AACA-96CF90E1007F

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.*	Evervault is responsible for the provision and secure management of services as described above, Connections into and out of the CDE which are managed by Evervault happen at the AWS layer. The environment overall is based across multiple AWS regions and multiple Availability Zones within each region. Each Region has a public facing zone, and an internal zone, and is designed in line with the AWS well architected framework. Inbound connectivity to the environment is only via the publicly exposed APIs. Customers of Evervault services always retain the responsibility for determination of their own Third-Party Service Providers, such as PSPs with whom they share CHD. This is included in the Demarcation of Responsibilities and managed by the customer via the In Scope Evervault App by the customer.
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)
AWS Data Centers	2	North Virginia, USA, US East 1 Dublin, Ireland EU West 1

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

Docusign Envelope ID: 85E51032-77A0-4DF9-AACA-96CF90E1007F

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.

* 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.

Docusign Envelope ID: 85E51032-77A0-4DF9-AACA-96CF90E1007F

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, Inc. (AOC 01/30/2025, v4.0.1)	Public Cloud Services Provider
Cloudflare Inc (AOC 03/12/2025, v4.0.1)	Cloud Services, DNS, Web Application Firewall, VPN, DDOS Software as a Service
Cybersource Corporation (AOC 08/07/2024, v4.0)	PAN intermediary for the provision of Network Tokens
3dsecure.io (PCI 3DS Core Security Standard, v1.0, 05/22/2025)	CHD – backup provider in support of 3DS service resilience

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

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

Docusign Envelope ID: 85E51032-77A0-4DF9-AACA-96CF90E1007F

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: Messaging Platform

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

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	1.2.6 - No insecure services, protocols, or ports are allowed in Evervault Environment. 1.3.3 - Evervault did not support wireless environments that connect to the CDE. 1.4.4 - Evervault did not directly store CHD. 2.2.5 - No insecure services, protocols, or ports are allowed in Evervault CDE. 2.3.1, 2.3.2 - Evervault did not support wireless environments that connect to the CDE.

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

Docusign Envelope ID: 85E51032-77A0-4DF9-AACA-96CF90E1007F

	3.2.1, 3.5.1, 3.5.1.1, 3.5.1.2, 3.5.1.3 – Evervault did not store CHD. 3.3.3 - Evervault was not an issuer and did not support issuing services. 3.4.1 - Evervault did not display cardholder data. 3.4.2 - Evervault did not store CHD and therefore did not have remote access to full PAN data. 3.7.2 – Evervault did not distribute cryptographic keys. 3.7.6 – Evervault did not utilize cleartext cryptographic key-management operations. 3.7.9 – Evervault did not distribute keys. 4.2.1.2 - There were no wireless networks permitted for transmitting cardholder data. 4.2.2 - Evervault did store CHD and therefore was not able to send PAN via end-user messaging technologies. 6.4.1 – This requirement was superseded by Requirement 6.4.2 as of 31-March-2025. 6.4.3 – Evervault was not responsible for payment page script configuration management. 7.2.6 - Evervault did not store CHD. 8.2.2 - Shared authentication credentials were not used in Evervault CDE. 8.2.3 - Evervault did not have remote access to customer premises. 8.2.7 - No entities were provided with remote access to the CDE. 8.6.2- All application access was via assigned and named user accounts. 9.4.1-9.4.7 - Evervault did not store CHD on physical media. 9.5.1, 9.5.1.1, 9.5.1.2, 9.5.1.2.1, 9.5.1.3 - Evervault was not responsible for the management of card reading devices. 10.2.1.1 – Evervault did not store CHD. 10.4.3 - No exceptions or anomalies were identified. 10.7.1 – This requirement was superseded by Requirement 10.7.2 as of 31-March-2025. 11.2.2 - Evervault did not support wireless access points within the cardholder data environment. 11.4.5, 11.4.6 – Evervault did not rely on network segmentation to isolate the CDE. 11.4.7 - Evervault clients are not required to perform external penetration testing of the services they use from Evervault. 11.6.1 - Evervault was not responsible for payment page script configuration management. Req A2.1.1-A2.1.3 – Evervault did not support the use of SSL or early TLS. Req A3 – Evervault was not a DESV.
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.

Docusign Envelope ID: 85E51032-77A0-4DF9-AACA-96CF90E1007F

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.*	05/09/2025
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	07/18/2025
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.

Docusign Envelope ID: 85E51032-77A0-4DF9-AACA-96CF90E1007F

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 July 21, 2025.

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 ***Evervault 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 *Not Applicable* has not demonstrated compliance with PCI DSS requirements.

Target Date for Compliance: *Not Applicable*

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 *Not Applicable* 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
Not Applicable.	Not Applicable.
Not Applicable.	Not Applicable.

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

Docusign Envelope ID: 85E51032-77A0-4DF9-AACA-96CF90E1007F

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

DocuSigned by:
John Hetherton
E01EF682BA6049A...

Signature of Service Provider Executive Officer ↑	Date: 7/25/2025
Service Provider Executive Officer Name: **John Hetherton**	Title: **Head of Compliance**

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:

DocuSigned by:
Kevin Whalen
0B32514137D7445...

Signature of Lead QSA ↑	Date: 7/25/2025
Lead QSA Name: **Kevin Whalen**	

DocuSigned by:
Kevin Whalen
0B32514137D7445...

Signature of Duly Authorized Officer of QSA Company ↑	Date: 7/25/2025
Duly Authorized Officer Name: **Kevin Whalen**	QSA Company: **Prescient Security LLC**

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.

Docusign Envelope ID: 85E51032-77A0-4DF9-AACA-96CF90E1007F

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.