Docusign Envelope ID: F440D60F-36BD-444F-B97A-ECD2E77F8677



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: F440D60F-36BD-444F-B97A-ECD2E77F8677

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

Entity Name: Conferma

Date of Report as noted in the Report on Compliance: 23-Jan-2026

Date Assessment Ended: 16-Jan-2026

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

Docusign Envelope ID: F440D60F-36BD-444F-B97A-ECD2E77F8677

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:	Conferma Limited
DBA (doing business as):	Conferma
Company mailing address:	Ocean House, Towers Business Park, Wilmslow Rd, Didsbury, Manchester, M20 2RY, UK
Company main website:	www.conferma.com
Company contact name:	Rik Kay
Company contact title:	CISO
Contact phone number:	+44 7741377357
Contact e-mail address:	rikkay@conferma.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:	NCC Group Security Services Ltd.
Company mailing address:	XYZ Building, 2 Hardman Boulevard, Spinningfields, Manchester, M3 3AQ, UK.
Company website:	www.nccgroup.com
Lead Assessor name:	Francis Bell
Assessor phone number:	+44 7800 603130
Assessor e-mail address:	Francis.Bell@nccgroup.com

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

Docusign Envelope ID: F440D60F-36BD-444F-B97A-ECD2E77F8677

Assessor certificate number:	200-822

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:	Conferma API, Conferma Online, Conferma Connect, Conferma mobile app

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	Financial Technology (Fintech) services. Supporting payment and management of travel and expenses through the issuing of virtual credit card numbers (VCNs) and reconciliation services that allows clients to track expenses and payments made by individual travellers.	
☐ 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):		

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.

Docusign Envelope ID: F440D60F-36BD-444F-B97A-ECD2E77F8677

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.	Conferma facilitate the issuing of virtual credit cards used for card not present payments through the following Conferma products: **Conferma API** – Allows deployment of virtual cards using the customers own systems interfacing with the Conferma API. **Conferma Online** – Website accessible externally that provides the payment card details on request to authorised users (either travel management companies

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

Docusign Envelope ID: F440D60F-36BD-444F-B97A-ECD2E77F8677

	or the banks who manage the individual customers). The website offers the functionality to request, amend, **Conferma Connect** – Used where hotels require the sending of the payment card to accept a booking. Conferma Connect creates a card image containing the card data which is sent electronically to the hotel. Conferma uses a third-party PCI DSS certified fax service (Concord) to send some of the card details. **Conferma mobile app** – Allows customers to view the virtual card to be able to use the card details for eCommerce transactions and to add the card to a mobile device's wallet for use for contactless payments.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Conferma provide services that facilitate the issuing of virtual credit cards for travel management companies to support travel related bookings for corporate travellers. The platform provided by Conferma facilitates the payment and management of corporate travel through the issuing of virtual credit card numbers (VCNs). The VCNs are generated by issuing banks and the Conferma platform provides subsequent reconciliation services that allows Conferma's clients to track their individual traveller's expenses and travel bookings.
Describe system components that could impact the security of account data.	Conferma provide services that facilitate the issuing of virtual credit cards for travel management companies and end-corporates to support business expenses for corporate customers. Cardholder data is received and processed within the Conferma platform between issuing banks and third party travel booking companies using both APIs to interface directly with client systems and through public facing web applications. Conferma store the PAN for the virtual credit cards in databases and receive and process the card verification code and expiry date from the issuers. The platform also provides for the transmission of cardholder data via third party fax bureau services (for smaller merchants who do not have systems that can interface via the API method) and who require cardholder data provided via fax as part of their business process. Conferma is not a merchant but are a service provider for the purposes of PCI DSS. Conferma provide the platform that acts as an interface between the card issuers and the travel management companies. This allows Conferma's customers to make travel bookings, but Conferma does not make bookings on the platform itself or generate VCNs. Instead, the platform performs routing of details between the travel management companies and third-party booking platforms where customers can use their virtual card details directly on the third party booking systems.

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

Docusign Envelope ID: F440D60F-36BD-444F-B97A-ECD2E77F8677

	Where Conferma's platform stores, processes, and transmits cardholder data to third parties (e.g., via fax, APIs or Conferma's own secure email solution) this is for the purposes of providing details to secure bookings but does not involve payment processing. A 'transaction' for Conferma consists of the receipt, transformation and transmission of the card details from the issuer to the client. All cards issued on behalf of Conferma's issuing banks are virtual cards with no printing of physical plastic cards.

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

Docusign Envelope ID: F440D60F-36BD-444F-B97A-ECD2E77F8677

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.*	Conferma provide services that facilitate the issuing of virtual credit cards for travel management companies to support travel related bookings for corporate travellers. Conferma facilitates the booking, payment and management of travel and expenses through the issuing of virtual credit card numbers (VCNs) and reconciliation services that allow its clients to track expenses and payments made by individual travellers. Conferma's virtual card platform interfaces between travel management companies, issuers and banks to provide for the issuing of the VCNs.
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)
Data centres	2	London, United Kingdom Maidenhead, United Kingdom
Data centres	2	Microsoft Azure Regions: UK South UK West

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

Docusign Envelope ID: F440D60F-36BD-444F-B97A-ECD2E77F8677

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: F440D60F-36BD-444F-B97A-ECD2E77F8677

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:
Concord	Concord transmits account data to merchant companies where fax services are required.
Fortra/AlertLogic	No account is shared with Forta/AlertLogic. Conferma make use of the Forta/AlertLogic service for logging and monitoring SIEM and SOC services.
CloudFlare	Web Application Firewall service
Iomart	No account data is shared with iomart. The data centres hosting the CDE are managed by iomart.
Microsoft Azure	No account data is shared with Azure. The CDE is hosted in Azure as the Cloud Service Provider.
SplunkCloud	No account data is shared with SplunkCloud. Logs are retained in SplunkCloud as the previous SIEM service until such time that 12 months logs will be held in Fortra/AlertLogic.

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: Conferma API, Conferma Online, Conferma Connect, Conferma mobile app

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.

Docusign Envelope ID: F440D60F-36BD-444F-B97A-ECD2E77F8677

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	2.3.1 & 2.3.2 - Review of the scope of the environment confirmed there are no wireless networks connected to the CDE or transmitting account data. 3.3.1.1 - Review of business processes and observation of transaction data confirmed that track data is not received. 3.3.1.3 - Review of business processes and observation of transaction data confirmed that PIN and PIN block data is not received. 3.5.1.2 & 3.5.1.3 – Disk-level or partition-level encryption is not used. 3.6.1.3 & 3.7.6 - Review of key management processes and interviews confirmed that there are no cleartext cryptographic key components in scope. 3.7.2 & 3.7.9 Review of the process for the use of PGP keys confirmed that only the public key is exported and provided to clients. There is no other distribution of keys. 4.2.1.2 - Review of the scope of the environment confirmed there are no wireless networks connected to the CDE or transmitting account data. 5.2.3 & 5.2.3.1 - Review of the scope of this assessment confirms that all systems are either Microsoft Windows based systems, that already include anti-malware software or are appliance-based devices that do not support the deployment of anti-malware software. 6.4.1 - As per the guidance in PCI SSC FAQ 1593, this requirement is not applicable as it has been superseded by 6.4.2 after 31 March 2025 6.4.3 – Review of the scope of this assessment confirms there are no payment pages in scope. 8.2.3 - Review of the scope of services provide confirms that Conferma do not have remote access to customer premises. 8.3.9 & 8.3.10.1 - Review of the implementation of MFA confirms that MFA is required for access to all system components. 8.3.10 - As per the guidance in PCI SSC FAQ 1593, this requirement is not applicable as it has been superseded by 8.3.10.1 after 31 March 2025. 8.6.1 & 8.6.2 - Review of the service and application accounts defined in Active Directory confirmed they have been configured to prevent interactive login. 9.4.1.1 & 9.4.1.2 - Review of the scope of this assessment confirms there are no offline media backups in scope. 9.4.2 - Review of the scope of this assessment confirms there is no media to be classified. 9.4.3 & 9.4.4 - Review of the scope of this assessment confirms that media is not distributed outside of the hosted environments. 9.4.5 & 9.4.5.1 - Review of the scope of this assessment confirms that media is not stored on removable or external electronic media that would require an inventory log.

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

Docusign Envelope ID: F440D60F-36BD-444F-B97A-ECD2E77F8677

	9.4.6 - Review of the scope of this assessment confirms that there is no hard-copy material with account data in scope. all 9.5.x - Review of the scope of this assessment confirms there are no POI devices in scope. 10.4.2 & 10.4.2.1 - Interviews confirmed that all system components are treated with the same level of importance and reviewed daily. 10.7.1 - As per the guidance in PCI SSC FAQ 1593, this requirement is not applicable as it has been superseded by 10.7.2 after 31 March 2025 11.4.7 - Review of the scope of this assessment confirms that Conferma do not provide multi-tenant services. 11.6.1 – Review of the scope of this assessment confirms there are no payment pages in scope. 12.3.2 - The customised approach has not been used to meet any requirements.
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: F440D60F-36BD-444F-B97A-ECD2E77F8677

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-Jan-2026
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	16-Jan-2026
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: F440D60F-36BD-444F-B97A-ECD2E77F8677

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 23-Jan-2026)*.

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 *Conferma* 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.

Docusign Envelope ID: F440D60F-36BD-444F-B97A-ECD2E77F8677

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:
Richard Kay
50748586E52942D...

Signature of Service Provider Executive Officer ↑	Date: 23-Jan-26
Service Provider Executive Officer Name: Rik Kay	Title: CISO

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: Not applicable

DocuSigned by:
Francis Bell
8B6F0BFD791746A...

Signature of Lead QSA ↑	Date: 23-Jan-26
Lead QSA Name: Francis Bell	

DocuSigned by:
Stephen Higgins
67DB2BB1F5604E1...

Signature of Duly Authorized Officer of QSA Company ↑	Date: 23-Jan-26
Duly Authorized Officer Name: Stephen Higgins	QSA Company: NCC Group Security Services 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.

Docusign Envelope ID: F440D60F-36BD-444F-B97A-ECD2E77F8677

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.