Docusign Envelope ID: 1E765104-2324-8D14-8242-F5EEBE74486D



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: 1E765104-2324-8D14-8242-F5EEBE74486D

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

Entity Name: Mercury Technologies

Date of Report as noted in the Report on Compliance: March 13, 2026

Date Assessment Ended: March 13, 2026

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

Docusign Envelope ID: 1E765104-2324-8D14-8242-F5EEBE74486D

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:	Mercury Technologies
DBA (doing business as):	
Company mailing address:	660 Mission St, Floor 4, San Francisco, CA 94117
Company main website:	https://mercury.com
Company contact name:	Shannon Ingelsby
Company contact title:	Senior Program Manager, Compliance Governance & Oversight
Contact phone number:	937-751-3506
Contact e-mail address:	singlesby@mercury.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):	
Qualified Security Assessor	
Company name:	TCM Security, Inc
Company mailing address:	1380 Rio Rancho Blvd SE #184, Rio Rancho, NM 87124
Company website:	https://tcm-sec.com
Lead Assessor name:	Bradley Thornton
Assessor phone number:	877-243-6690
Assessor e-mail address:	brad.thornton@educate360.com
Assessor certificate number:	206-657

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

Docusign Envelope ID: 1E765104-2324-8D14-8242-F5EEBE74486D

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:	Mercury	
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:	None	
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:		

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.	Mercury operates as a service intermediary between start-up companies and banks, offering fintech services and account management, including dispute resolution and account reconciliations, on behalf of the start-ups. Importantly, Mercury does not handle Cardholder Data (CHD) directly. They establish a direct link with Mastercard through Mastercard Connect, from which they receive files potentially containing Primary Account Number (PAN) data alongside other non-CHD information. Mercury's role necessitates only the non-CHD data for their processing tasks, but they cannot influence the content of the files sent by Mastercard.

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

Docusign Envelope ID: 1E765104-2324-8D14-8242-F5EEBE74486D

	To manage these files, Mercury utilizes a dedicated laptop that is exclusively connected to Mastercard for the purpose of processing the received files. Mercury's process involves extracting the necessary non-CHD information and then securely eliminating the PAN data from these files, creating a new file devoid of any PAN data for their internal use. The original files containing PAN data are securely erased shortly after their reception. Throughout this process, the files containing PAN data are strictly confined to the laptop, ensuring they do not leave the device.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Not applicable
Describe system components that could impact the security of account data.	Not applicable

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

Docusign Envelope ID: 1E765104-2324-8D14-8242-F5EEBE74486D

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.*	Review of environment and how CHD is processed, stored, and transmitted
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*
Not Applicable – Entity does not have a CDE	Not Applicable	Not Applicable

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

Docusign Envelope ID: 1E765104-2324-8D14-8242-F5EEBE74486D

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.

Docusign Envelope ID: 1E765104-2324-8D14-8242-F5EEBE74486D

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:
Lithic	Lithic provides card issuing and payment processing services, enabling businesses to create and manage virtual and physical payment cards. For Mercury, Lithic facilitates transaction processing, card issuance, and account management, ensuring secure and compliant handling of payment data.

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

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

Docusign Envelope ID: 1E765104-2324-8D14-8242-F5EEBE74486D

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: Mercury

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: 1E765104-2324-8D14-8242-F5EEBE74486D

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	1.3.3 – No wireless networks in the CDE 1.4.4 – Cardholder data is not stored 2.2.5 – Insecure services are not used 2.3.1 – Wireless does not exist in the CDE 2.3.2 – Wireless does not exist in the CDE 3.1.1 – CHD is not retained or stored 3.1.2 – CHD is not retained or stored 3.3.1-3.3.3 – SAD is not stored or received 3.4.1 – CHD is not retained or stored 3.4.2 – CHD is not retained or stored 3.5.1 – CHD is not retained or stored 3.6.1 – CHD is not retained or stored 3.7.1-3.7.9 – CHD is not retained or stored 4.1.1 – Public networks are not used to transmit CHD 4.1.2 – Public networks are not used to transmit CHD 4.2.1.2 – Wireless does not exist in the CDE 4.2.2 - PANs are never sent by end-user messaging technology 5.2.3.1 - All system components are continuously protected and none deemed not at risk 5.3.2.1 - All system components are continuously scanned 5.3.3 - Removable media is not used 6.2.1-6.2.4 - Entity does not develop software 6.3.2 - Entity does not develop software or use bespoke or custom software 6.4.1-6.5.6 - Entity does not use public-facing web applications in the CDE 7.2.6 - CHD is not retained or stored 8.2.3 - Entity does not have remote access to customers 8.2.7 - Vendors are not allowed access to the cardholder environment 8.3.10 - Entity does not control customer passwords 8.3.10.1 - Entity does not control customer passwords 9.2.3 - Wireless does not exist in the CDE 9.3.2-9.3.4 - Visitors are not allowed in sensitive areas 9.4.1 - Media is not used 9.4.1.1 - Media is not used 9.4.1.2 - Media is not used 9.4.2-9.4.5 - Media is not used 9.4.5.1 - Media is not used 9.4.6 – Hard-copy materials are not used 9.4.7 – Media is not used 9.5.1 - Entity does not manage POI devices 9.5.1.1 - Entity does not manage POI devices 9.5.1.2 - Entity does not manage POI devices 10.4.2.1 - All log reviews are considered in requirement 10.4.1

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

Docusign Envelope ID: 1E765104-2324-8D14-8242-F5EEBE74486D

	11.2.1 - Wireless does not exist in the CDE 11.2.2- Wireless does not exist in the CDE 11.3.1.1 - All vulnerabilities are considered and addressed by 6.3.1 11.3.2 - Client does not have an external presence into the CDE 11.3.2.1 - Client does not have an external presence into the CDE 11.4.1-11.4.7 - Client does not have an external presence into the CDE 11.6.1 - Organization does not have payment pages 12.3.1 - No targeted risk analysis required as they are addressed within requirements or not applicable. 12.10.4.1 - All requirements met within requirement 12.3.1
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: 1E765104-2324-8D14-8242-F5EEBE74486D

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.*	2026-02-16
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	2026-03-13
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: 1E765104-2324-8D14-8242-F5EEBE74486D

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 2026-03-13)*.

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 *(*Mercury*)* 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: 1E765104-2324-8D14-8242-F5EEBE74486D

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:
Branden Wagner
6C9FFD3862BF473...

Signature of Service Provider Executive Officer ↑	Date: 3/24/2026
Service Provider Executive Officer Name: Branden Wagner	Title: Head of Information Security

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:

Bradley Thornton

Signature of Lead QSA ↑	Date: 2026-03-13
Lead QSA Name: Bradley Thornton	

Alex Tushinsky

Signature of Duly Authorized Officer of QSA Company ↑	Date: 2026-03-13
Duly Authorized Officer Name: Alex Tushinsky	QSA Company: TCM Security

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: 1E765104-2324-8D14-8242-F5EEBE74486D

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.