# Payment Card Industry
# Data Security Standard

## Attestation of Compliance for Report on Compliance – Service Providers

**Version 4.0**

Revision 2

Publication Date: August 2023

# PCI DSS v4.0 Attestation of Compliance for Report on Compliance – Service Providers

**Entity Name: Tyler Technologies**

**Assessment End Date: December 19th, 2024**

**Date of Report as noted in the Report on Compliance: December 20th, 2024**

# 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: | Tyler Technologies |
| DBA (doing business as): | Tyler Technologies |
| Company mailing address: | 5101 Tennyson Parkway, Plano, TX 75024 |
| Company main website: | Https://www.tylertech.com |
| Company contact name: | Jeffrey Newball |
| Company contact title: | Manager InfoSec Compliance |
| Contact phone number: | 1-888-529-8248 |
| Contact e-mail address: | Jeffrey.newball@tylertech.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): | N/A |
| Qualified Security Assessor | |
| Company name: | International Business Machines (IBM) |
| Company mailing address: | New Orchard Rd, Armonk, New York, 10504 |
| Company website: | www.ibm.com |
| Lead Assessor name: | Karl Kakadelis |

| | |
|---|---|
| Assessor phone number: | 864-978-5914 |
| Assessor e-mail address: | Karl.Kakadelis@ibm.com |
| Assessor certificate number: | QSA 753-294 |

## 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: | Tyler Online Gateway Access (TOGA), Tyler Capital(TC), and Tyler Payments(TP) |

Type of service(s) assessed:

| | | |
|---|---|---|
| **Hosting Provider:**<br>☐ Applications / software<br>☐ Hardware<br>☐ Infrastructure / Network<br>☐ Physical space (co-location)<br>☐ Storage<br>☐ Web-hosting services<br>☐ Security services<br>☐ 3-D Secure Hosting Provider<br>☐ Multi-Tenant Service Provider<br>☐ Other Hosting (specify): | **Managed Services:**<br>☐ Systems security services<br>☐ IT support<br>☐ Physical security<br>☐ Terminal Management System<br>☐ Other services (specify): | **Payment Processing:**<br>☐ POI / card present<br>☒ Internet / e-commerce<br>☐ MOTO / Call Center<br>☐ ATM<br>☐ 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.*

## 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: | Physical Security (AWS), Merchant Services is under another Assessment |

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: | Physical Services are handled by third party AWS and the merchant services for the entity are assessed under another assessment. |

### Part 2b. Description of Role with Payment Cards (ROC Section 2.1)

| | |
|---|---|
| Describe how the business stores, processes, and/or transmits account data. | Tyler Online Gateway Access (TOGA): All transactions for this business function are a passthrough web-based transaction which transmits data securely to Chase Paymentech's Payment Gateway. Chase handles all the authorization and payment processes. Authorizations are returned to the transaction originator upon receipt from Chase. Cardholder data is not retained. Tyler Capital (TC): The Insite Web Portal |

| | |
|---|---|
| | collects customer payment and credit card information and initiates a secure session to the credit card processor for authorization. Once authorization is received, Insite posts the credit card transaction details in the Insite secure database.  Eden/Tyler Payments (TP): Takes credit card payments without the consuming application directly handling any in-scope PCI DSS credit card data. Consumers enter their credit card information directly into the hosted Tyler Payments cloud platform via secure frames within their browser (iFrames). |
| Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data. | As a service provider, Tyler Technologies receives cardholder data from their customers' locally installed applications and processes them on their behalf. No cardholder data is stored post authorization for Eden/Tyler Payments or TOGA. Tyler Capital (TC) stores the credit card number to facilitate re-occurring payments. This credit card information is encrypted in a database within the CDE. |
| Describe system components that could impact the security of account data. | This PCI DSS assessment covers TOGA, Tyler Capital and Eden/Tyler Payments web applications. No CHD is stored for TOGA and Eden. CHD is encrypted by the web application using ASP.NET and for Tyler Capital is stored in SQL DB. The isolated and segmented Tyler Technologies PCI environment is hosted in the AWS cloud. The CDE is composed of Windows web and DB servers, AWS firewall, router and switches; with connectivity to the Chase payment gateway. |

## Part 2. Executive Summary *(continued)*

### Part 2c. Description of Payment Card Environment

| | |
|---|---|
| Provide a high-level description of the environment covered by this Assessment.<br>*For example:*<br>• *Connections into and out of the cardholder data environment (CDE).*<br>• *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.*<br>• *System components that could impact the security of account data.* | Tyler Online Gateway Access (TOGA): All transactions for this business function are a passthrough web-based transaction which transmits data securely to Chase Paymentech's Payment Gateway. Chase handles all the authorization and payment processes. Authorizations are returned to the transaction originator upon receipt from Chase. Cardholder data is not retained.<br>Tyler Capital (TC): The Insite Web Portal collects customer payment and credit card information and initiates a secure session to the credit card processor for authorization. Once authorization is received, Insite posts the credit card transaction details in the Insite secure database.<br>Eden/Tyler Payments (TP): Takes credit card payments without the consuming application directly handling any in-scope PCI DSS credit card data. Consumers enter their credit card information directly into the hosted Tyler Payments cloud platform via secure frames within their browser (iFrames).<br>As a service provider, Tyler Technologies receives cardholder data from their customers' locally installed applications and processes them on their behalf. No cardholder data is stored post authorization for Eden/Tyler Payments or TOGA. Tyler Capital (TC) stores the credit card number to facilitate re-occurring payments. This credit card information is encrypted in a database within the CDE.<br>This PCI DSS assessment covers TOGA, Tyler Capital and Eden/Tyler Payments web applications. No CHD is stored for TOGA and Eden. CHD is encrypted by the web application using ASP.NET and for Tyler Capital is stored in SQL DB. The isolated and segmented Tyler Technologies PCI environment is hosted in the AWS cloud. The CDE is composed of Windows web and DB servers, AWS firewall, router and switches; with connectivity to the Chase payment gateway. |
| Indicate whether the environment includes segmentation to reduce the scope of the Assessment.<br>(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**<br>(How many locations of this type are in scope) | **Location(s) of Facility**<br>(city, country) |
|---|---|---|
| *Example: Data centers* | *3* | *Boston, MA, USA* |
| AWS | 2 | US-EAST and US-WEST |
| Corporate Office | 1 | Plano Texas |
| | | |
| | | |
| | | |
| | | |

## 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 |
|---|---|---|---|---|
| | | | | YYYY-MM-DD |
| | | | | 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, Payment Applications (PA-DSS), Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, and Contactless Payments on COTS (CPoC) solutions.

## 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:** |
|---|---|
| AWS | IaaS |
| Paymentech LLC | Payment Gateway |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

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

## 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:* Tyler Online Gateway Access (TOGA), Tyler Capital(TC), and Tyler Payments(TP)

| PCI DSS Requirement | Requirement Finding<br>More than one response may be selected for a given requirement. Indicate all responses that apply. | | | | Select If Below Method(s) Was Used | |
|---|---|---|---|---|---|---|
| | In Place | Not Applicable | Not Tested | Not in Place | Customized Approach | Compensating Controls |
| 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. | 2.3.1 - No wireless in scope<br>3.2.1 - N/A 2024<br>3.3.2 - N/A 2024<br>3.3.3 - N/A 2024<br>3.4.2 - N/A PAN never Decrypted<br>3.5.1.1 -N/A 2024<br>3.5.1.2 - N/A 2024<br>3.6.1.1 N/A 2024<br>3.7.9 - N/A Keys never provided to customers<br>4.2.1.1 -N/A2024<br>5.2.1- N/A2024<br>5.2.3.1 - N/A2024<br>5.3.2.1 - N/A2024<br>5.3.3 - N/A 2024<br>6.3.2 - N/A 2024<br>6.4.1 - N/A 2024<br>6.4.2 -N/A 2024<br>6.4.3 -N/A 2024<br>6.5.2 - N/A New infrastructure<br>7.2.4 N/A 2024<br>7.2.5 - N/A 2024<br>7.2.5.1 -N/A 2024<br>8.3.10 - No Access is granted to customers to the CDE is given<br>8.5.1 N/A 2024<br>8.6.1- N/A 2024<br>8.6.2 - N/A 2024<br>8.6.3 - N/A 2024<br>9.2.1.1. - No Physical Locations<br>9.3.4 - No Physical Locations<br>9.5.1.1 - No Physical Locations<br>9.5.1.2 - No Physical Locations<br>9.5.1.2.1 - No Physical Locations<br>9.5.1.3 - No Physical Locations<br>10.4.2.1 - N/A 2024<br>10.7.2 - N/A 2024<br>10.7.3 - N/A 2024<br>10.7.3 - N/A 2024<br>11.2.1 - No Wireless in Scope<br>11.2.2 - No Wireless in Scope<br>11.3.1.1 - N/A 2024<br>11.3.1.2 - N/A 2024<br>11.4.7 - N/A 2024<br>11.5.1.1 - N/A 2024<br>11.6.1 - N/A 2024<br>12.3.1 - N/A 2024<br>12.3.2 - N/A 2024 |

| | |
|---|---|
| | 12.3.3 - N/A 2024<br>12.3.4 - N/A 2024<br>12.5.2.1 - N/A 2024<br>12.5.3 - N/A 2024<br>12.6.2 - N/A 2024<br>12.6.3.1 - N/A 2024<br>12.6.3.2 - N/A 2024<br>12.10.4.1 - N/A 2024<br>12.10.5 - N/A 2024<br>12.10.7 - N/A 2024 |
| For any Not Tested responses, identify which sub-requirements were not tested and the reason. | |

# Section 2 Report on Compliance

(**ROC Sections 1.2 and 1.3.2**)

| | | | |
|---|---|---|---|
| Date Assessment began:<br>***Note:*** *This is the first date that evidence was gathered, or observations were made.* | | | 2024-10-2 |
| Date Assessment ended:<br>***Note:*** *This is the last date that evidence was gathered, or observations were made.* | | | 2024-12-19 |
| Were any requirements in the ROC unable to be met due to a legal constraint? | | | ☐ Yes ☒ No |
| Were any testing activities performed remotely?<br>If yes, for each testing activity below, indicate whether remote assessment activities were performed: | | | ☒ Yes ☐ No |
| • Examine documentation | ☒ Yes | ☐ No | |
| • Interview personnel | ☒ Yes | ☐ No | |
| • Examine/observe live data | ☒ Yes | ☐ No | |
| • Observe process being performed | ☒ Yes | ☐ No | |
| • Observe physical environment | ☒ Yes | ☐ No | |
| • Interactive testing | ☒ Yes | ☐ No | |
| • Other: | ☐ Yes | ☐ No | |

# 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 2024-12-20)*.

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 Tyler Technologies 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 |
|---|---|
| | |
| | |
| | |

## 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 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:
Jeremy Ward
565FA51EA72D4D9...

| | |
|---|---|
| *Signature of Service Provider Executive Officer ↑* | Date: 2024-12-20 |
| Service Provider Executive Officer Name: Jeremy Ward | Title: Chief Information Security Officer |

### 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.<br>If selected, describe all role(s) performed: |

Signed by:
Karl Kakadelis
3018AE50A4B4424...

| | |
|---|---|
| *Signature of Lead QSA ↑* | Date: 2024-12-20 |
| Lead QSA Name: Karl Kakadelis | |

DocuSigned by:
Gil Eng
7C536C10D4464BD...

| | |
|---|---|
| *Signature of Duly Authorized Officer of QSA Company ↑* | Date: 2024-12-20 |
| Duly Authorized Officer Name: Gil Eng | QSA Company: IBM |

### 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.<br>If selected, describe all role(s) performed: |

## 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 | ☒ | ☐ | |