
# Payment Card Industry (PCI)
# Data Security Standard

## Attestation of Compliance for Onsite Assessments – Service Providers

**Version 3.2.1**

Revision 2

September 2022

# Document Changes

| Date | Version | Description |
|---|---|---|
| September 2022 | 3.2.1<br>Revision 2 | Updated to reflect the inclusion of UnionPay as a Participating Payment Brand. |

# Section 1: Assessment Information

### *Instructions for Submission*

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS).* Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

| **Part 1. Service Provider and Qualified Security Assessor Information** | | | | | |
|---|---|---|---|---|---|
| **Part 1a. Service Provider Organization Information** | | | | | |
| Company Name: | Cloud Software Group, Inc. | | DBA (doing business as): | | |
| Contact Name: | Meghan Hester | | Title: | Senior Director of IT Governance and Business Operations | |
| Telephone: | (800) 424-8749 | | E-mail: | Meghan.Hester@cloud.com | |
| Business Address: | 851 W Cypress Creed Rd | | City: | Fort Lauderdale | |
| State/Province: | FL | Country: | USA | Zip: | 33309 |
| URL: | https://cloud.com | | | | |

| **Part 1b. Qualified Security Assessor Company Information (if applicable)** | | | | | |
|---|---|---|---|---|---|
| Company Name: | risk3sixty, LLC | | | | |
| Lead QSA Contact Name: | Jeremy Brandt | | Title: | Senior Associate | |
| Telephone: | 404-717-2778 | | E-mail: | Jeremy.Brandt@risk3sixty.com | |
| Business Address: | 408 S Atlanta St, Suite 180 | | City: | Roswell | |
| State/Province: | GA | Country: | USA | Zip: | 30075 |
| URL: | https://risk3sixty.com | | | | |

## Part 2. Executive Summary

### Part 2a. Scope Verification

**Services that were INCLUDED in the scope of the PCI DSS Assessment** (check all that apply):

| Name of service(s) assessed: | ShareFile | |
|---|---|---|
| Type of service(s) assessed: | | |
| **Hosting Provider:**<br>☒ Applications / software<br>☐ Hardware<br>☐ Infrastructure / Network<br>☐ Physical space (co-location)<br>☒ Storage<br>☐ Web<br>☐ Security services<br>☐ 3-D Secure Hosting Provider<br>☐ Shared Hosting Provider<br>☐ Other Hosting (specify): | **Managed Services (specify):**<br>☐ Systems security services<br>☐ IT support<br>☐ Physical security<br>☐ Terminal Management System<br>☐ Other services (specify): | **Payment Processing:**<br>☐ POS / 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): File upload, download and exchange service | | |

***Note**: These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.*

| **Part 2a. Scope Verification** *(continued)* | | |
|---|---|---|
| **Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment** (check all that apply): | | |
| Name of service(s) not assessed: | Not Applicable | |
| Type of service(s) not assessed: | | |
| **Hosting Provider:**<br>☐ Applications / software<br>☐ Hardware<br>☐ Infrastructure / Network<br>☐ Physical space (co-location)<br>☐ Storage<br>☐ Web<br>☐ Security services<br>☐ 3-D Secure Hosting Provider<br>☐ Shared Hosting Provider<br>☐ Other Hosting (specify): | **Managed Services (specify):**<br>☐ Systems security services<br>☐ IT support<br>☐ Physical security<br>☐ Terminal Management System<br>☐ Other services (specify): | **Payment Processing:**<br>☐ POS / 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): | | |
| Provide a brief explanation why any checked services were not included in the assessment: | Not Applicable | |

| Part 2b. Description of Payment Card Business | |
|---|---|
| Describe how and in what capacity your business stores, processes, and/or transmits cardholder data. | ShareFile service may incidentally store or transmit cardholder data due to how its customers utilize the ShareFile service. ShareFile customers upload and download files that, in theory, could contain CHD. During the intended use of the ShareFile product, it may store customer files and transmit files containing CHD. |
| Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data. | ShareFile stores customer files at rest with unique per file encryption keys (AES 256 with HMACSHA256) which is provided to AWS S3 via HTTPS for server-side encryption (SSE-C protocol). ShareFile protects CHD in transit by managing and maintaining web certificates that enforce strong cryptography (TLS_AES_128_GCM_SHA256, with TLS v1.2 or higher) for connections over the internet.<br><br>Since the SF product falls into the security impacting category of PCI service provider profiles, ShareFile provides a PCI compliant service to satisfy its customers' PCI compliance expectations of their third-party service providers. ShareFile provides a customer facing PCI responsibility management matrix that delineates ShareFile's PCI responsibilities as assessed within this audit, what is a shared responsibility with customers, or entirely a customer PCI responsibility. ShareFile customers are ultimately responsible for their own PCI compliance. |

**Part 2c. Locations**

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

| Type of facility: | Number of facilities of this type | Location(s) of facility (city, country): |
|---|---|---|
| *Example: Retail outlets* | *3* | *Boston, MA, USA* |
| Not Applicable - ShareFile's assessed environment is hosted with AWS | Not Applicable | Not Applicable |
| | | |
| | | |
| | | |
| | | |
| | | |

## Part 2d. Payment Applications

Does the organization use one or more Payment Applications? ☐ Yes ☒ No

Provide the following information regarding the Payment Applications your organization uses:

| Payment Application Name | Version Number | Application Vendor | Is application PA-DSS Listed? | PA-DSS Listing Expiry date (if applicable) |
|---|---|---|---|---|
| Not Applicable | Not Applicable | Not Applicable | ☐ Yes ☐ No | Not Applicable |
| | | | ☐ Yes ☐ No | |
| | | | ☐ Yes ☐ No | |
| | | | ☐ Yes ☐ No | |
| | | | ☐ Yes ☐ No | |
| | | | ☐ Yes ☐ No | |
| | | | ☐ Yes ☐ No | |
| | | | ☐ Yes ☐ No | |

## Part 2e. Description of 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 POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.* | ShareFile provides file uploads/downloads/exchange services to and from ShareFile's platform, hosted in AWS, that may contain Account Data. ShareFile customer file contents that may contain Account Data are uploaded or downloaded from the internet over HTTPS. File uploads routed to AWS CloudFront, and subsequently encrypted and stored in S3 buckets. Larger or multiple file downloads and uploads are handled by the Content Streamer. File contents uploaded are passed to CloudAV microservice, which scans decrypted customer files for malicious software. Further, file contents and file metadata are served to the Content Indexer microservice and ingested by ElasticSearch/OpenSearch clusters, which indexes files for easy search functionality. All transmissions in this flow are transmitted via TLS v.1.2 or higher. |
| Does your business use network segmentation to affect the scope of your PCI DSS environment?<br>*(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)* | ☐ Yes ☒ No |

| Part 2f. Third-Party Service Providers | |
|---|---|
| Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated? | ☐ Yes ☒ No |
| ***If Yes:*** | |
| Name of QIR Company: | Not Applicable |
| QIR Individual Name: | Not Applicable |
| Description of services provided by QIR: | Not Applicable |
| Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated? | ☐ Yes ☒ No |
| ***If Yes:*** | |

| **Name of service provider:** | **Description of services provided:** |
|---|---|
| Not Applicable | Not Applicable |
| | |
| | |
| | |
| | |
| | |

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

## Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as "Not Tested" or "Not Applicable" in the ROC.
- **None** – All sub-requirements of that requirement were marked as "Not Tested" and/or "Not Applicable" in the ROC.

For all requirements identified as either "Partial" or "None," provide details in the "Justification for Approach" column, including:

- Details of specific sub-requirements that were marked as either "Not Tested" and/or "Not Applicable" in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

***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:** | ShareFile |
|---|---|

| **PCI DSS Requirement** | **Details of Requirements Assessed** | | | |
|---|---|---|---|---|
| | **Full** | **Partial** | **None** | **Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.) |
| Requirement 1: | ☐ | ☒ | ☐ | **1.2.2 -N/A- Risk3sixty reviewed network diagrams and network configuration for the SF environment to verify that all in scope systems are within the AWS data centers. As per the AWS responsibility matrix, it is the responsibility of the cloud service provider to maintain router and network flow controls for PCI DSS** |
| Requirement 2: | ☐ | ☒ | ☐ | **2.1.1 -N/A- No wireless environments are in use or connected to the CDE**<br>**2.2.3 -N/A- no insecure services, daemons, or protocols are in use**<br>**2.6 -N/A- ShareFile is not a shared hosting provider** |
| Requirement 3: | ☐ | ☒ | ☐ | **3.2 -N/A- ShareFile is not an issuer and does not support issuing services**<br>**3.4.1 -N/A- Disk encryption is not used**<br>**3.6.6 - N/A- Manual clear-text cryptographic key-management opeartions are not used** |
| Requirement 4: | ☐ | ☒ | ☐ | **4.1.1 -N/A- No wireless environments are in use or connected to the CDE**<br>**4.2 -N/A- End user messaging technologies are not used to send CHD** |

| | | | | |
|---|---|---|---|---|
| Requirement 5: | ☐ | ☒ | ☐ | **5.1.2 -N/A- All ShareFile systems in scope have Microsoft Defender for Endpoint installed on them** |
| Requirement 6: | ☐ | ☒ | ☐ | **6.4.3 -N/A- ShareFile does not use live PAN data within testing or development environments**<br>**6.4.6 -N/A- No significant changes apply since it is ShareFile's initial PCI DSS compliance assessment** |
| Requirement 7: | ☒ | ☐ | ☐ | |
| Requirement 8: | ☐ | ☒ | ☐ | **8.1.5 -N/A- No access is provisioned with third party personnel**<br>**8.5.1 -N/A - ShareFile does not have remote access into customer premises**<br>**8.7 -N/A- Risk3sixty reviewed network and dataflow diagrams and observed CHD data store inventories to verify that Elasticsearch and AWS OpenSearch are not traditional databases and does not apply to 8.7** |
| Requirement 9: | ☐ | ☐ | ☒ | **9 -N/A- Physical security controls are the responsibility of ShareFile's CSPs** |
| Requirement 10: | ☒ | ☐ | ☐ | |
| Requirement 11: | ☐ | ☒ | ☐ | **11.1 -N/A- Risk3sixty reviewed network diagrams and network configurations to verify that no wireless infrastructure can connect to or impact the security of the assessed environment and is not in scope for this assessment**<br>**11.2.3.a -N/A- ShareFile is undergoing its first PCI DSS validation attempt, and there are no significant changes from previous PCI assessments**<br>**11.3.4 -N/A- Segmentation is not used to isolate the CDE from other networks** |
| Requirement 12: | ☒ | ☐ | ☐ | |
| Appendix A1: | ☐ | ☐ | ☒ | **N/A - ShareFile is not a shared hosting provider** |
| Appendix A2: | ☐ | ☐ | ☒ | **N/A - ShareFile does not use SSL/early TLS for POS POI terminal connections** |

## Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

| | | |
|---|---|---|
| The assessment documented in this attestation and in the ROC was completed on: | *11/30/2023* | |
| Have compensating controls been used to meet any requirement in the ROC? | ☒ Yes | ☐ No |
| Were any requirements in the ROC identified as being not applicable (N/A)? | ☒ Yes | ☐ No |
| Were any requirements not tested? | ☐ Yes | ☒ No |
| Were any requirements in the ROC unable to be met due to a legal constraint? | ☐ Yes | ☒ No |

# Section 3: Validation and Attestation Details

## Part 3. PCI DSS Validation

**This AOC is based on results noted in the ROC dated *11/30/23.***

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

| | |
|---|---|
| ☒ | **Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *CSG-ShareFile* has demonstrated full compliance with the PCI DSS. |
| ☐ | **Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *CSG-ShareFile* has not demonstrated full compliance with the PCI DSS.<br>**Target Date** for Compliance:<br>An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with the payment brand(s) before completing Part 4.* |
| ☐ | **Compliant but with Legal exception:** One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.<br>*If checked, complete the following:* |

| Affected Requirement | Details of how legal constraint prevents requirement being met |
|---|---|
| | |
| | |

## Part 3a. Acknowledgement of Status

**Signatory(s) confirms:**

***(Check all that apply)***

| | |
|---|---|
| ☒ | The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version *v3.2.1*, and was completed according to the instructions therein. |
| ☒ | All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects. |
| ☐ | I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization. |
| ☒ | I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times. |
| ☒ | If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply. |

| Part 3a. Acknowledgement of Status (continued) | |
|---|---|
| ☒ | No evidence of full track data[1], CAV2, CVC2, CVN2, CVV2, or CID data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment. |
| ☒ | ASV scans are being completed by the PCI SSC Approved Scanning Vendor *Qualys* |

**Part 3b. Service Provider Attestation**

DocuSigned by:
Meghan Hester
4B3AF3A90AFF4CC...

| | |
|---|---|
| *Signature of Service Provider Executive Officer* ↑ | *Date:* 12/1/2023 |
| *Service Provider Executive Officer Name:* **Meghan Hester** | *Title:* **Senior Director of IT Governance and Business Operations** |

**Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)**

| | |
|---|---|
| If a QSA was involved or assisted with this assessment, describe the role performed: | *Jeremy Brandt (QSA) performed scope validation, interviews and observations, evidence gathering, and report generation* |

DocuSigned by:
D150591D733C4C5...

| | |
|---|---|
| *Signature of Duly Authorized Officer of QSA Company* ↑ | *Date:* 12/1/2023 |
| *Duly Authorized Officer Name:* Jeremy Brandt | *QSA Company:* risk3sixty, LLC |

**Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)**

| | |
|---|---|
| If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed: | *Not Applicable* |

[1] Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

[2] The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

[3] Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

## Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

*Check with the applicable payment brand(s) before completing Part 4.*

| 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 a firewall configuration to protect cardholder data | ☒ | ☐ | |
| 2 | Do not use vendor-supplied defaults for system passwords and other security parameters | ☒ | ☐ | |
| 3 | Protect stored cardholder data | ☒ | ☐ | |
| 4 | Encrypt transmission of cardholder data across open, public networks | ☒ | ☐ | |
| 5 | Protect all systems against malware and regularly update anti-virus software or programs | ☒ | ☐ | |
| 6 | Develop and maintain secure systems and applications | ☒ | ☐ | |
| 7 | Restrict access to cardholder data by business need to know | ☒ | ☐ | |
| 8 | Identify and authenticate access to system components | ☒ | ☐ | |
| 9 | Restrict physical access to cardholder data | ☒ | ☐ | |
| 10 | Track and monitor all access to network resources and cardholder data | ☒ | ☐ | |
| 11 | Regularly test security systems and processes | ☒ | ☐ | |
| 12 | Maintain a policy that addresses information security for all personnel | ☒ | ☐ | |
| Appendix A1 | Additional PCI DSS Requirements for Shared Hosting Providers | ☒ | ☐ | |
| Appendix A2 | Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections | ☒ | ☐ | |