



Payment Card Industry (PCI) Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

June 2018

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:	Genpact Wilkes Barre	DBA (doing business as):	
Contact Name:	Sandeep Srivastava	Title:	Assistant Vice President – Information Security
Telephone:	+919643807147	E-mail:	Sandeep.Srivastava2@genpact.com
Business Address:	335 New Commerce Blvd	City:	Wilkes Barre
State/Province:	Pennsylvania	Country:	USA
		Zip:	18706
URL:	https://www.genpact.com		

Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:	ControlCase LLC		
Lead QSA Contact Name:	Kamlesh Naidu	Title:	PCI QSA
Telephone:	+1 703.483.6383	E-mail:	knaidu@controlcase.com
Business Address:	12015 Lee Jackson Memorial Hwy, Suite 520	City:	Fairfax
State/Province:	VA	Country:	USA
		Zip:	22033
URL:	https://www.controlcase.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:	Genpact Wilkes Barre Process provides support services to AFL, Penske, Ralph Lauren, Abbott, Audacy for processes handling CHD data at Wilkes Barre location.
------------------------------	---

Type of service(s) assessed:

Hosting Provider:

- ☐ Applications / software
- ☐ Hardware
- ☐ Infrastructure / Network
- ☐ Physical space (co-location)
- ☐ Storage
- ☐ Web
- ☐ Security services
- ☐ 3-D Secure Hosting Provider
- ☐ Shared Hosting Provider
- ☐ Other Hosting (specify):

Managed Services (specify):

- ☐ Systems security services
- ☐ IT support
- ☐ Physical security
- ☐ Terminal Management System
- ☐ Other services (specify):

Payment Processing:

- ☐ POS / 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): Business Process 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: None

Type of service(s) not assessed:

Hosting Provider:

- ☐ Applications / software
- ☐ Hardware
- ☐ Infrastructure / Network
- ☐ Physical space (co-location)
- ☐ Storage
- ☐ Web
- ☐ Security services
- ☐ 3-D Secure Hosting Provider
- ☐ Shared Hosting Provider
- ☐ Other Hosting (specify):

Managed Services (specify):

- ☐ Systems security services
- ☐ IT support
- ☐ Physical security
- ☐ Terminal Management System
- ☐ Other services (specify):

Payment Processing:

- ☐ POS / 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 Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.

Genpact Wilkes Barre Process provides support services to AFL, Penske, Ralph Lauren, Abbott, Audacy for processes handling CHD data at Wilkes Barre location.

Genpact Wilkes Barre supports various lines of businesses for the following customers:

Penske

Ralph Lauren

AFL

Audacy

Abbott

Penske

Process

	<p>Genpact agents handle inbound calling of Customer Payments for Penske.</p> <p>Customer calls Genpact Analyst to make payment on their account.</p> <p>Analyst enters credit card information into Rental Net (Penske Payment Portal).</p> <p>If a receipt is required by the customer, it is emailed to them, only last 4 digits of CC are visible.</p> <p>Genpact agents also perform outbound calling to existing Rental and Lease customers as part of collections process.</p> <p>Genpact agents also perform outbound calling to late stage accounts assignments as part of collections process. Call recording is not performed.</p> <p>Storage</p> <p>There is no storage of cardholder data for Penske process.</p> <p>Transmission</p> <p>Genpact connects to Penske via IPSEC VPN over Internet channel.</p> <p>Ralph Lauren</p> <p>Process</p> <p>Genpact analyst handle out/inbound calling of Customer Payments for Ralph Lauren.</p> <p>Customer calls Genpact Analyst to make payment on their account.</p> <p>Analyst enters credit card information (PAN, Type of CC, Name on Card, Expiry Date) into Payeezy (Customer Payment Portal for USA) (https://globalgateway4.firstdata.com/) and Bambora (https://web.na.bambora.com/admin/sDefault.asp) (Customer Payment Portal for Canada) (CVV is required for Canada and is not required for USA)</p> <p>If a receipt is required by the customer, it is emailed, only last 4 digits of CC are visible.</p> <p>No Calls are recorded in Genpact for Ralph Lauren process.</p> <p>Storage</p> <p>There is no storage of cardholder data for Ralph Lauren process.</p>
--	--

	<p>Transmission</p> <p>Genpact agent connect to Genpact VPN over SSL VPN with TLS 1.2 AES encryption.</p> <p>Genpact agents use Link (https://globalgatewaye4.firstdata.com/ and https://web.na.bambora.com/admin/sDefault.asp) provided by Ralph Lauren over Internet channel for customer payments.</p> <p>AFL</p> <p>Process</p> <p>Genpact agents handle inbound calling of Customer Payments for AFL.</p> <p>Genpact Analyst apply payment to which invoices using Cardholder Data (PAN, Name, Expiry Date) provided by customer.</p> <p>Cardholder Data (PAN, Name, Expiry Date) is entered https://cardpointe.cardconnect.com by Genpact analyst.</p> <p>Storage</p> <p>There is no storage of cardholder data for AFL process.</p> <p>Transmission</p> <p>Genpact connects to AFL over IPSEC VPN Channel.</p> <p>Genpact agent connect to Genpact VPN over SSL VPN with TLS 1.2 AES encryption.</p> <p>Genpact agents connect to https://cardpointe.cardconnect.com for Payment completions for AFL process.</p> <p>Audacy</p> <p>Process</p> <p>Genpact agents handle inbound and outbound calls along with Emails while supporting Audacyfor Collections process.</p> <p>Genpact analyst will need to login into Audacy managed remote environment with to perform Collection process.</p> <p>While handling inbound calls, Customers with preexisting balances call in to the analysts to make payments. Genpact analysts log in to payment portal and asks customer to provided cardholder data (PAN, Exp date, Cardholder Name) and performs the</p>
--	---

payment. Genpact analyst can view only last 4 digits of PAN after payment has been completed.

While handling outbound calls, List generated out of Genpact Cora on outstanding balances. Analyst makes call to customer. Genpact analysts log in to payment portal and asks customer to provided cardholder data (PAN, Exp date, Cardholder Name) and performs the payment. Genpact analyst can view only last 4 digits of PAN after payment has been completed.

While handling emails, Genpact receives emails from customers containing Credit Card Authorization forms which has cardholder data information (Full PAN, Expiry, Name) and customer signature (auth purposes). Genpact analysts log in to payment portal and performs the payment with cardholder data provided by customer. Genpact analyst can view only last 4 digits of PAN after payment has been completed.

Storage

There is no storage of cardholder data for Audacyprocess.

Transmission

Genpact connects to Audacy over IPSEC VPN Channel and via MPLS Channel.

Abbott

There is no storage processing or transmission of Cardholder data.

Genpact also provides work from home for above mentioned processes. Users connect to Genpact environment using Genpact remote VPN. Users then login Genpact Citrix and provide the payment support services mentioned above. SoftPhones are accessed from Genpact User workstation and payment is performed using Internet Browser application from Citrix.

The assessor noted that all applications and tools used to process, host card information are hosted in client environment or managed by client. The assessor noted that no Genpact owned, managed or hosted tools applications are used for hosting or processing CHD information. No CHD information is stored at Genpact as part of Genpact Wilkes Barre

	<p>process. However, Genpact agents have access to client information and can view cardholder data (PAN, Cardholder Name, CVV and Expiry) on client-hosted applications and this is considered as transmission of cardholder data.</p> <p>Genpact only provides the agents with workstation access and network connectivity to AFL, Penske, Ralph Lauren, Abbott, Audacy managed applications.</p>
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	<p>Genpact provides business process service to AFL, Penske, Ralph Lauren, Abbott, Audacyfor supporting their processes which involve cardholder data.</p> <p>Genpact does not store cardholder data for Genpact Wilkes Barres processes.</p> <p>Genpact agents use Link (https://globalgatewaye4.firstdata.com/ and https://web.na.bambora.com/admin/sDefault.asp) provided by Ralph Lauren over Internet channel for customer payments.</p> <p>Genpact agents connect to https://cardpointe.cardconnect.com for Payment completions for AFL process.</p> <p>Genpact connects to AFL over IPSEC VPN Channel.</p> <p>Genpact connects to Penske via IPSEC VPN over Internet channel.</p> <p>Genpact connects to Audacyover IPSEC VPN Channel and via MPLS Channel.</p>

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):
<i>Example: Retail outlets</i>	3	<i>Boston, MA, USA</i>
Process Floors	1	Genpact Wilkes Barre, 335 New Commerce Blvd, Wilkes Barre, PA 18706
Data Center	1	Genpact Wilkes Barre, 335 New Commerce Blvd, Wilkes Barre, PA 18706
AWS Cloud	1	Mumbai-India
Azure Cloud	1	India

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)
			<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	

Part 2e. Description of 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 POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.

The covered infrastructure for Genpact Wilkes Barre certification includes following:

- MPLS Links for Genpact Backbone connectivity
- Network Components like Palo Alto Firewall and IPS, Cisco Switch, Cisco Internal Router, Cisco MPLS Router, Cisco VPN Router, Cisco VPN Firewall
- Windows Servers like Domain Controller, Patch, Antivirus, File Server
- Citrix Systems like NetScaler
- QRadar SIEM
- Agent Workstations
- Genpact connectivity to Audacy, Abbott over MPLS channel.
- Genpact connectivity to Penske, Audacy over IPSEC VPN channel.
- Genpact Remote VPN Connectivity over SSL VPN for AFL and Ralph Lauren Process

The assessor noted that few services used by Genpact Wilkes Barre environment is covered under other Genpact PCI-DSS AOCs.

Genpact Capital One PCI-DSS Certification dated 15 December 2020

for

TACACS

NTP Servers

IBM Qradar

Genpact CWT-WFH SAQ-D dated 31 July 2020

for

	CrowdStrike Antivirus	
	Genpact NAB PCI-DSS Certification dated 19 April 2021. for Domain controller OKTA Server	
	Databank Holdings, LLC. AOC dated 25 Oct 2020 Location 400 S Akard Street Dallas, TX 75202 Data Center Physical Security	
	CyrusOne LLC AOC dated 14 August 2020 Location 209 7th Street West, Cincinnati, OH 45202 Data Center Physical Security	
	AWS hosting provider AOC dated 14 December 2020 Zone Locations Mumbai-India	
	Azure hosting provider AOC dated 3 May 2021 Zone Locations India	
Does your business use network segmentation to affect the scope of your PCI DSS environment? <i>(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)</i>		<input checked="" type="checkbox"/> Yes <input type="checkbox"/> 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?		<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
If Yes:		
Name of QIR Company:		

QIR Individual Name:		
Description of services provided by QIR:		
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?		<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
If Yes:		
Name of service provider:	Description of services provided:	
DataBank Holdings	Third Party Data Center	
CyrusOne LLC	Third Party Data Center	
Azure	Managed Hosting Provider	
Amazon Web Services	Managed Hosting Provider	
CrowdStrike	Managed Service Provider	
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:		Genpact Business Process Service for AFL, Penske, Ralph Lauren, Abbott, Audacy		
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:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1.2.3: Wireless Network is not being used in Genpact Wilkes Barre environment. Hence this control is not applicable. 1.3.1: There is no DMZ interface implemented for Genpact Wilkes Barre Environment. Hence this control is not applicable. 1.3.2: There is no DMZ interface implemented for Genpact Wilkes Barre. Hence this control is not applicable. 1.3.6: There is no cardholder data storage in Genpact Wilkes Barre environment. Hence this control is not applicable.
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2.1.1: Wireless Network is not being used in Genpact Wilkes Barre environment. Hence this control is not applicable. 2.2.3: There are no insecure services present in Genpact Wilkes Barre environment. Hence this control is not applicable. 2.6: Genpact Wilkes Barre is not providing any shared hosting services. Hence this control is not applicable.
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3.1, 3.4, 3.4.1, 3.5, 3.5.1, 3.5.2, 3.5.3, 3.5.4, 3.6, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7, 3.6.8: Genpact Wilkes Barre environment does not store cardholder data. Hence these controls are not applicable.

				<p>3.2: Genpact Wilkes Barre environment is neither an issuer nor does it support issuing services and also, does not receive sensitive authentication data. Hence, this control is not applicable.</p> <p>3.3: Genpact agents cannot view full or masked PAN in Genpact Wilkes Barre environment. Hence this control is not applicable.</p>
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>4.1.1: Wireless Network is not being used in Genpact Wilkes Barre environment. Hence this control is not applicable.</p> <p>4.2 - Cardholder data is not being transmitted over end user messaging services. Hence this control is not applicable.</p>
Requirement 5:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>5.1.2- Genpact Wikes Barre does not have any systems which are not considered commonly affected by malicious software. Hence, this control is not Applicable.</p>
Requirement 6:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>6.3, 6.3.1, 6.3.2, 6.4, 6.4.1, 6.4.2, 6.4.3, 6.4.4, 6.5, 6.5.1, 6.5.2, 6.5.3, 6.5.4, 6.5.5, 6.5.6, 6.5.7, 6.5.8, 6.5.9, 6.5.10: Genpact Wilkes Barre environment does not perform any in-house Software or Application development or host any application in its environment. Hence these controls are not applicable.</p> <p>6.4.6: No significant change occurred in Genpact Wilkes Barre environment within the past 12 months. Hence this control is not applicable.</p> <p>6.6: No internet facing application is hosted in Genpact Wilkes Barre environment. Hence this control is not applicable.</p>
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 8:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>8.1.5: No remote access is provided to the vendors in Genpact Wilkes Barre environment. Hence this control is not applicable.</p> <p>8.3.1: There is no non-console administrative access allowed into CDE of Genpact Wilkes Barre environment. Hence this control is not applicable.</p> <p>8.5.1: Genpact Wilkes Barre environment does not have remote access to customer premises. Hence this control is not applicable.</p> <p>8.7: Genpact Wilkes Barre environment does not host any databases which is storing cardholder data. Hence this control is not applicable.</p>
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>9.5, 9.5.1, 9.6, 9.6.1, 9.6.2, 9.6.3, 9.7, 9.7.1, 9.8.2: Cardholder data is not backed-up in external electronic media or tapes as part of Genpact Wilkes Barre environment. Hence these controls are not applicable.</p> <p>9.8, 9.8.1: Genpact Wilkes Barre doesn't have hard copies consisting PAN which need to be crosscut shredded, incinerated, or pulped. Hence these controls are not applicable.</p>

				9.9, 9.9.1, 9.9.2, 9.9.3: Card-present channel is not available in Genpact Wilkes Barre environment. There are no physical interaction devices capturing cardholder data in Genpact Wilkes Barre environment. Hence these controls are not applicable.
Requirement 10:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10.2.1: Genpact Wilkes Barre environment does not store cardholder data. Hence this control is not applicable.
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	11.1.1: Wireless Network is not being used in Genpact Wilkes Barre environment. Hence this control is not applicable. 11.2.3: There was no major or significant change in Genpact Wilkes Barre environment during the past one year. Hence this control is not applicable. 11.3.3: Exploitable vulnerabilities are not found during penetration testing in Genpact Wilkes Barre environment. Hence this control is not applicable.
Requirement 12:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	12.3.9: Genpact Wilkes Barre environment does not provide remote access to vendors and business partners. Hence this control is not applicable.
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Genpact Wilkes Barre environment is not a shared hosting provider. Hence all controls are not applicable.
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	A2: Genpact Wilkes Barre environment does not have any POS/POI Terminal. Hence this control is not applicable. A2.2: Genpact Wilkes Barre environment does not use SSL or early TLS version. Hence this control is not applicable. A2.3: Genpact Wilkes Barre environment does not have any insecure service in environment. Hence this control is not applicable.

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:	July 12, 2021	
Have compensating controls been used to meet any requirement in the ROC?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the ROC identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Were any requirements not tested?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated July 12, 2021.

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**):

<input checked="" type="checkbox"/>	<p>Compliant: All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby <i>Genpact Wilkes Barre</i> has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p>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 (<i>Service Provider Company Name</i>) has not demonstrated full compliance with the PCI DSS.</p> <p>Target Date for Compliance:</p> <p>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. <i>Check with the payment brand(s) before completing Part 4.</i></p>						
<input type="checkbox"/>	<p>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.</p> <p><i>If checked, complete the following:</i></p> <table border="1"> <thead> <tr> <th>Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met				
Affected Requirement	Details of how legal constraint prevents requirement being met						

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(**Check all that apply**)

<input checked="" type="checkbox"/>	The ROC was completed according to the <i>PCI DSS Requirements and Security Assessment Procedures</i> , Version 3.2.1, and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
<input type="checkbox"/>	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	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)

<input checked="" type="checkbox"/>	No evidence of full track data ¹ , CAV2, CVC2, CID, or CVV2 data ² , or PIN data ³ storage after transaction authorization was found on ANY system reviewed during this assessment.
<input checked="" type="checkbox"/>	ASV scans are being completed by the PCI SSC Approved Scanning Vendor ControlCase LLC

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	Date: July 12, 2021
Service Provider Executive Officer Name: Vidya Srinivasan	Title: Senior Vice President – Infrastructure, Enterprise Risk and Global Mobility

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

If a QSA was involved or assisted with this assessment, describe the role performed:	The QSA performed the assessment against the PCI DSS 3.2.1 standard at the assessed entity and documented the findings in the report on compliance.
--	---



Signature of Duly Authorized Officer of QSA Company ↑	Date: July 12, 2021
Duly Authorized Officer Name: Kamlesh Naidu	QSA Company: ControlCase 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:	
---	--

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

