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 India Pvt Ltd (McGraw Hill process)		DBA (doing business as):		
Contact Name:	Sandeep Srivastava		Title:	Assistant Vice President – Information Security	
Telephone:	+91-9643807147		E-mail:	sandeep.srivastava2@genpact.com	
Business Address:	Genpact India Private Ltd , Building No. 8,Raheja Mind Space Pocharam		City:	Secunderabad	
State/Province:	Telangana	Country:	India	Zip:	500088
URL:	https://www.genpact.com/				

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

Company Name:	Panacea Infosec Pvt. Ltd.				
Lead QSA Contact Name:	Himanshu Mishra		Title:	QSA	
Telephone:	+91 7738705367		E-mail:	himanshu@panaceainfosec.com	
Business Address:	Plot no-226, 3rd Floor, A-2, Sector - 17 Dwarka		City:	New Delhi	
State/Province:	Delhi	Country:	India	Zip:	110075
URL:	https://www.panaceainfosec.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 India Pvt Ltd (McGraw Hill process) provides backend support to McGraw Hill. The back-office services include reconciliation, settlement, chargeback, etc. Genpact agents also perform American Express card linking, card hot listing, card replacement for McGraw Hill.	
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): Genpact BPO Service to access applications hosted at McGraw Hill client network is accessed using Citrix session through IPsec over internet. All applications which are used for card functions or day to day operations in back office services are provided by McGraw Hill.		
***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: □ 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:	Not Applicable

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Genpact India Pvt. Ltd. henceforth referred as ‘Genpact’ is a global business process outsourcing company with its head office in India. Genpact is a leader in managing business processes, offering a broad portfolio of core enterprise and industry-specific services. It manages multiple client processes that are outsourced by their customers. PCI DSS scope for this assessment is the services provided to McGraw Hill by Genpact. Hence after McGraw Hill also referred as MHE. Genpact provides back office support services to McGraw Hill. Genpact has dedicated delivery centers for McGraw Hill and access to logical environment is controlled and managed by the McGraw Hill. Genpact has access to McGraw Hill’s environment depending upon the type of services it offers using MHE provided Citrix environment. Genpact is service provider to McGraw Hill for providing assistance in voice process, back-office services like reconciliation, settlement, chargeback, etc. Genpact agents also perform American Express card linking, card hot listing, card replacement for McGraw Hill users. Genpact agent's login to their local desktop using their individual AD credentials. Agents’ further login into client environment via Citrix using client provided credentials. Agents perform inbound and outbound for providing services to customers and taking payments. However, agents are not taking payments at this point of time as they are working from home due current worldwide COVID-19 pandemic situation. Agents also perform following activities: Card Linking: Agents perform linking of credit card(s) against individual’s profile from McGraw Hill in client’s environment in which multiple cards can be linked to individual’s ID. Agents can see full 14 digits American Express PAN before linking with ID. However, only last 4 visible post card linking in ERP application hosted and managed by client. Reconciliation: Agents perform two kinds of reconciliations in which first one involves the reconciliation of the cards linked to individual’s profile on ERP application. In case individual has left the organization, linked card is immediately unlinked/deleted. Secondly, agent perform the reconciliation of transactions performed by MHE personnel using linked credit cards. Reconciliation reports contains full PAN which are visible to agents in client environment and cannot be exported locally on agent’s desktop.

	Chargeback: Agents perform chargebacks using PSP no. for querying payment records. Full card no. is not present in the records received for chargeback data. Agents start with matching the amount and perform applicable investigations using evidence received. Amount will be reverted to credit cards in case the claim is legitimate otherwise amount will be deducted from the account. In case of frauds, agents will the raise the ticket to American Express provided portal and applicable investigations will be performed by AmEx. Amount will be refunded once the ticket is raised. However, the amount will be deducted again if the claim is found not to be correct. All the activities are performed the inside Citrix environment and no cardholder data is stored, processed or transmitted in Genpact's environment.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Genpact MHE agents at Pocharam, Hyderabad accesses the client hosted applications using Citrix session over IPsec configured over Internet. All the applications used in back-office services are provided by MHE and can only be accessible inside the Citrix session. The agents cannot cut, copy anything from Citrix environment to Genpact environment, Genpact Agents have only capability of view full Card numbers while linking the Amex card or other functions. Hence, Genpact MHE process does not have direct ability to impact the security of cardholder data.

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*
Process Floor	1	MHE Production Floor Genpact India Private Ltd, RITP SEZ, Building No. 8, Raheja Mind Space, MHE Production Floor at 5th floor Pocharam, Hyderabad, Telangana – 500088.
Data Center	3	Datacenter 1. Genpact, RITP SEZ, Building No. 8, Raheja Mind Space, MHE Production Floor at 5th floor Pocharam, Hyderabad, Telangana – 500088. 2. Genpact, 2nd floor 14-45, IDA Uppal, Opp. NGRI, Habsiguda, Uppal,

		Hyderabad, Telangana, India, Pin Code: 500039 3. Genpact, 1st floor DLF City - Phase V, Sector 53, Gurgaon - 122002, Haryana, 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)
Not Applicable	Not Applicabe	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. *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 assessment covered following areas: 1-Network devices (Palo Alto, Cisco Firewall, Cisco Router and Cisco core switch) and access rules on firewall. 2-Infrastructure servers (AD, AV, Patch Update, NTP, etc.) 3-Security servers (FIM, syslog server & log analyzer) 4-Dedicated operations floor & desktops used to access 'MHE Process' through client's applications 5.The connectivity from Genpact to MHE is configured through IPsec VPN over internet, the Genpact MHE agents access client MHE provided applications in Citrix environment. 6. VPN firewall, Cisco Firewall.

	7. Cisco ISE 8. IBM QRADAR

Does your business use network segmentation to affect the scope of your PCI DSS environment? *(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:**
STT Global data Centres India Pvt. Ltd.	Genpact Devices are hosted in Data Centers provided by STT Global. STT Global is PCI DSS certified entity and same has been validated by reviewen the PCI DSS AOC dated Oct 6th 2020.

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 India Pvt Ltd (McGraw Hill process) provides backend support to McGraw Hill.

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:	☐	☒	☐	1.2.3 The Control requires installation of perimeter firewalls between all wireless networks and the cardholder data environment. Since there is no wireless network in the assessed environment the control has been marked as not applicable. 1.3.6 The control requires placing of systems that store cardholder data in internal zone. For MHE process no card data is stored in the assessed environment hence, the control has been marked as not applicable.
Requirement 2:	☐	☒	☐	2.1.1 The control requires changing all wireless vendor defaults including installation but not limited to default wireless encryption keys, passwords, and SNMP community strings. Since there is no wireless network in the assessed environment the control has been marked as not applicable. 2.2.3 The control requires implementation of additional security features for any required services, protocols, or daemons that are considered to be insecure. Since no insecure services were found to be in use at Genpact (MHE Process) the control has been marked as not applicable.

				2.6 The control applies to shared hosting provider. Since Genpact (MHE Process) is not a shared hosting provider the control has been marked as not applicable
Requirement 3:	□	☒	□	3.1 The control applies to secure storage of cardholder data. Since there is no card data stored in the assessed environment the control has been marked as not applicable. 3.2 The control forbids storing sensitive authentication data after authorization. Since Genpact (MHE Process) neither receives nor stores sensitive authentication data the control has been marked as not applicable. 3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed): The card data is not stored. The assessor further noted that Genpact MHE agents can view card numbers in Customers MHE environment only. Hence this requirement is marked as not applicable. 3.4 Render PAN unreadable anywhere it is stored: There is no card data stored in Genpact MHE environment. Hence this requirement is marked as not applicable. 3.4.1 If disk encryption is used (rather than file- or column-level database encryption): It has been observed that disk encryption mechanism is not used at Genpact MHE Process. Hence this requirement is marked as not applicable. 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 These controls are related to key management of encryption keys. Since no card data is stored in the assessed environment encryption is not used and hence, controls related to key management have been marked as not applicable.
Requirement 4:	□	☒	□	4.1.1 The control applies to wireless networks transmitting cardholder data or connected to the cardholder data environment. Since there is no wireless network in the assessed environment the control has been marked as not applicable. 4.2 The control is for PANs be sent by end-user messaging technologies. Since there is no PANs being sent by end-user messaging technologies in the assessed environment the control has been marked as not applicable.
Requirement 5:	□	☒	□	Req 5.1.2 is not applicable as there are no systems in the scoped environment that are not commonly affected by malicious software.
Requirement 6:	□	☒	□	Req 6.3, 6.3.1 and 6.3.2 is not applicable as no software development or application development is done in the scoped environment.

				Req 6.4, 6.4.1, 6.4.2, 6.4.3 and 6.4.4 are not applicable as no software development or application development is done in the scoped environment. Req 6.4.6 is not applicable as there is no significant changes happened in Genpact MHE PCI DSS scope. Req 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 are not applicable as no software development or application development is done in the scoped environment. Req 6.6 is not applicable as no public facing applications were present to transmit/receive the cardholder data in the scoped environment.
Requirement 7:	☒	□	□	
Requirement 8:	□	☒	□	Req 8.1.5 is not applicable as remote access by third parties are not permitted in entities in scope environment. Req 8.5.1 is not applicable as Genpact MHE do not have any remote access to client (MHE) environment for managing any applications or systems. Req 8.6 is not applicable as entity does not have any other authentication mechanism for Genpact MHE process and associates in scope environment. Rea 8.7 is not applicable as entity does not have any database with card data for Genpact MHE process.
Requirement 9:	□	☒	□	Req 9.5, 9.5.1 – Genpact MHE does not use any removable media for backing up any cardholder data. Hence the control is not applicable. Req 9.6,9.7, 9.8 (including all sub requirement) – Genpact MHE does not use any removable media for backing up any cardholder data. Hence the control is not applicable. Req 9.8 (including all sub requirement) Genpact MHE does not use any removable media including CDs, DVDs, Tapes, USB, paper receipt, paper reports, and faxes for storing any data from cardholder data environment. Hence this requirement is not applicable Req 9.9, 9.9.1, 9.9.1. a, 9.9.1.b, 9.9.1.c,9.9.2, 9.9.2.a, 9.9.2.b, 9.9.3, 9.9.3.a, 9.9.3.b – There is no POS in Genpact MHE PCI DSS environment, hence this requirement is not applicable.
Requirement 10:	□	☒	□	10.2.1 This control requires logging of all individual access to card data. Since there is no card data stored in the assessed environment, the control has been marked as not applicable.

Requirement 11:	☐	☒	☐	Req 11.1.1 is not applicable as no wireless access points are present in entities in scope environment.
Requirement 12:	☐	☒	☐	Req 12.3.9 (including sub requirement): Genpact MHE does not provide remote access to the PCI DSS scope to any vendors or any other external entities. Hence the control is not applicable.
Appendix A1:	☐	☐	☒	Genpact MHE is not a shared hosting provider. Hence the requirement is not applicable.
Appendix A2:	☐	☐	☒	A 2.1 – Genpact MHE does not have POS terminals in its environment. Hence this requirement is not applicable. A2.2 – Genpact MHE does not use any SSL or early TLS protocol in the environment. Hence, this requirement is not Applicable. A2.3 – Genpact MHE does not have any POS/POI offering service and also does not provide any insecure IT services hence the requirement 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:	June 14th 2021	
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 (June 14th 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):***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby (Genpact India Pvt Ltd (McGraw Hill process)) 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 *(Service Provider Company Name)* has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: 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. *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 *(*3.2.1*)*, 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, CID, or CVV2 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 (ControlCase LLC.)

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	*Date:* June 14th 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

Himanshu

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* June 14th 2021
Duly Authorized Officer Name: Himanshu Mishra	*QSA Company:* Panacea Infosec Pvt. Ltd.

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	☒	□	