COMCAST ENTERPRISE SERVICES
PRODUCT-SPECIFIC ATTACHMENT
STANDARD AND ADVANCED SOFTWARE-DEFINED WIDE AREA NETWORKING

ATTACHMENT IDENTIFIER: SD-WAN, Version 3

The following additional terms and conditions are applicable to Sales Orders for Comcast's Standard and Advanced SD-WAN Services:

DEFINITIONS

Capitalized terms not otherwise defined herein shall have the meaning ascribed to them in the General Terms and Conditions.

"**Advanced SD-WAN Service**" includes the Standard SD-WAN Service plus the additional features described in Section 1.A. of Schedule A-1.

"**Architectural Confirmation Document**" or "**ACD**" means a document that contains the initial configuration for the SD-WAN Services, as agreed to by Customer and Comcast.

"Comcast System" means applications, websites, computing assets, systems, databases, devices, products, or services owned or operated by or for Comcast.

"Customer Expectations Document" means a document created by Comcast that identifies Comcast's and Customer's responsibilities and obligations with respect to the delivery and support of the Services.

"Customer System" means any of Customer's or Customer's subcontractor's(s') applications, websites, computing assets, systems, databases, devices, products, or services that process Comcast data.

"Estimated Availability Date" means the target Service Commencement Date for the Service.

"Information Security Standards" means the standards prescribed for use by the National Institute of Standards and Technology, aligned with the International Organization for Standardization/International Electrotechnical Commission 27000 series of standards.

"SD-WAN" means Software-defined Wide Area Network.

"Service(s)" for purposes of this PSA means the Standard and/or Advanced SD-WAN Services, as applicable.

"**Standalone**" means an optional configuration feature of the Advanced SD-WAN Service as described in Section 1.A. of Schedule A-1.

"**Standard SD-WAN Service**" means the Standard SD-WAN Service as described in Section 1.B. of Schedule A-1.

"**Underlay Service**" means the connectivity over which the Service operates.

ARTICLE 1. SERVICES

This attachment shall apply to Standard and Advanced SD-WAN Services. A further description of these Services is set forth in Schedule A-1 hereto, which is incorporated herein by reference.

ARTICLE 2. PROVIDER

The Services shall be provided by Comcast Business Communications, LLC or its applicable subsidiaries or Affiliates ("**Comcast**").

ARTICLE 3. SERVICE PROVISIONING INTERVAL

Following Customer's acceptance of a Sales Order, Comcast shall notify Customer of the Estimated Availability Date applicable to that Sales Order. Comcast shall use commercially reasonable efforts to provision the Service on or about the Estimated Availability Date; provided, however, that Comcast's failure to provision Service by said date shall not constitute a breach of the Agreement.

ARTICLE 4. SERVICE COMMENCEMENT DATE

The Service Commencement Date shall be the date Comcast informs Customer that the Service is available and performing at a minimum of two (2) Service Locations (or one (1) Service Location, in the case of Standalone). Charges for the Services shall begin to accrue on the Service Commencement Date.

ARTICLE 5. TERMINATION CHARGES; PORTABILITY

5.1 The charges set forth or referenced in each Sales Order have been extended to Customer in reliance on the Service Term.

5.2 Termination Charges.

A. Subject to Sections 5.2(C) and 5.2(D), in the event that a Service is terminated following Comcast's acceptance of the applicable Sales Order, but prior to the Service Commencement Date, Customer shall pay Termination Charges equal to one hundred and twenty percent (120%) of the costs and expenses incurred by Comcast in installing or preparing to install the Service.

B. Subject to Sections 5.2(C) and 5.2(D), in the event that a Service is terminated on or following the Service Commencement Date, but prior to the end of the applicable Service Term, Customer shall pay Termination Charges equal to a percentage of the monthly recurring Service charges remaining for the unexpired portion of the then-current Service Term, calculated as follows:

i 100% of the monthly recurring charges with respect to months 1-12 of the Service Term; plus
ii 80% of the monthly recurring charges with respect to months 13-24 of the Service Term; plus
iii 65% of the monthly recurring charges with respect to months 25 through the end of the Service Term.

Termination Charges shall be immediately due and payable upon cancellation or termination, and shall be in addition to any and all accrued and unpaid charges for the Service rendered by Comcast through the date of such cancellation or termination.

C. Exclusions. Termination Charges shall not apply to Service(s) terminated by Customer as a result of Comcast's material and uncured breach in accordance with the General Terms and Conditions.

D. Customer acknowledges and agrees that termination of the Comcast-provided Underlay Service shall constitute a termination of the Services and Customer shall pay Termination Charges with respect to the Services as provided herein; provided, that, if Customer terminated such Underlay Service as a result of Comcast's material and uncured breach in accordance with the General Terms and Conditions applicable hereto, then Customer will not be obliged to pay Termination Charges with respect to the Service.

5.3 Portability. Customer may terminate an existing Service (an "**Existing Service**") and turn up a replacement Service (*i.e.*, activate Service at a different Service Location) (a "**Replacement Service**") without incurring Termination Charges with respect to the Existing Service, provided that: (a) the Replacement Service must have a Service Term equal to or greater than the remaining Service Term of the Existing Service, but in no event less than twelve (12) months; (b) the Replacement Service must have monthly recurring charges equal to or greater than the monthly recurring charges for the Existing Service; (c) Customer submits a Sales Order to Comcast for the Replacement Service within ninety (90) days after termination of the Existing Service and that Sales Order is accepted by Comcast; (d) Customer reimburses Comcast for any and all installation charges that were waived with respect to the Existing Service; and (e) Customer pays the actual costs incurred by Comcast in installing and provisioning the Replacement Service.

ARTICLE 6. SD-WAN CUSTOMER PORTAL

Comcast provides Customer with access to a password-protected web portal for the purpose of accessing information regarding Customer's Service. The portal also provides a view of certain network-related data, subject to the availability of the Service.

ARTICLE 7. TECHNICAL SPECIFICATIONS; SERVICE LEVEL AGREEMENT

The technical specifications applicable to the Services are set forth in Schedule A-1 hereto. The service level agreement applicable to the Services is set forth in Schedule A-2 hereto. Comcast strives to achieve all service levels from the start of the SOW. However, Comcast is contractually relieved of the service level agreement set forth in Schedule A-2 and any service level requirements specified in SOWs for the first ninety (90) days immediately following the Service Commencement Date at any Service Location. Any remedies, including service level credits, set forth in Schedule A-2 and, where applicable, in any SOW shall be the Customer's sole and exclusive remedy for any failure to meet the specified service levels.

ARTICLE 8. PAYMENT CARD INDUSTRY COMPLIANCE

Subject to the terms outlined herein and below, the Services provided under this PSA are compliant with the current Payment Card Industry Data Security Standard ("**PCI DSS**") as set forth by the PCI Security Standards Council®. The Attestation of Compliance ("**AOC**") is limited to Comcast applications, software, infrastructure, network, and IT support of the SD-WAN with unified security (Versa Unified Threat Management) and Universal Customer Premises Equipment ("**uCPE**") provided by Comcast. All other Comcast Equipment and Customer-Provided Equipment are outside the scope of the AOC.

The obligations of each Party are outlined in the Responsibility Matrix set forth in Appendix A-3 to this PSA. Any variance to the Responsibility Matrix shall be identified in the ACD. Any Customer failure to meet an obligation set forth in the Responsibility Matrix, and/or any change to the Services may result in the Services no longer being deemed compliant with PCI DSS.

For clarity, PCI DSS compliance is ultimately the responsibility of the Customer. Comcast does not store, process, or transmit cardholder data on behalf of Customer or its end users in delivery of the Services, nor does Comcast have access to Customer's or its end users' cardholder data, the protection of which is the sole responsibility of Customer. Customer is responsible for security issues resulting from Customer change requests that deviate from Comcast's compliant configuration and all changes should be reviewed and documented through the Customer's internal change order process for PCI purposes and the configuration should be validated by the Customer's auditor for Customer to ensure PCI DSS compliance. Comcast cannot provide PCI DSS compliance-related guidance or advice on any Customer-requested changes to the Services as Customer is responsible for its own network operation and internal processes.

COMCAST ENTERPRISE SERVICES
PRODUCT-SPECIFIC ATTACHMENT SOFTWARE DEFINED WIDE AREA NETWORKING

SCHEDULE A-1
SERVICE DESCRIPTIONS AND TECHNICAL SPECIFICATIONS

The Services will be provided in accordance with the service descriptions and technical specifications set forth below:

1. Service Descriptions

A. **Advanced SD-WAN Service**. Advanced SD-WAN Service includes the Standard SD-WAN Service features described in Section 1.B. as well as the following additional features:

i. Comcast will create a custom configuration for Customer's Service based on the Customer-approved ACD.
ii. Following the Service Commencement Date, Comcast will provide Customer with a Service Location birth certificate which will include service details and test results; and during the first thirty (30) days after the Service Commencement Date, Comcast will provide Customer with a curation period during which Comcast will perform network tuning to Customer's SD-WAN Service.
iii. The Advanced SD-WAN Service configuration response objectives set forth in Section 5.E.i. below.
iv. The Advanced SD-WAN Service may be configured as Standalone. Standalone is an optional configuration feature that enables the Advanced SD-WAN Service to be provisioned, with or without the need for Service Location-to-Service Location or IPSec Tunnels to Third Party Peer topologies (as described in Section 4(C) below).

B. **Standard SD-WAN Service.** Standard SD-WAN Service is available only to Customers that have an active subscription to the Standard SD-WAN Service under a Sales Order entered into prior to September 26, 2022, this Service provides a secure connection, both point-to-point and point-to-multi-point, creating an encrypted overlay network to Customer's Underlay Service, regardless of whether such Underlay Service is provided by Comcast or a third party. SD-WAN Service enables network abstraction and the separation of the control plane and data plane. The following features are also included with SD-WAN Service:

i. SD-WAN Service is agnostic as to WAN transport technologies.
ii. Automatic and dynamic routing and load balancing of application traffic across multiple WAN connections based on business and application policies set by Customer.
iii. SD-WAN Service assists with the management, configuration, and orchestration of WANs.
iv. SD-WAN Service provides secure VPNs and has the ability to integrate additional network services and offload Internet-destined traffic closer to the edge of the network.
v. SD-WAN Service monitors the uCPE and circuits for "up/down" status, and alerts Customers based on configuration.
vi. 24x7 phone support.
vii. Access to the Portal (defined below), which provides analytics that show the performance and utilization of the Customer's network applications and elements.

2. Service Requirements

In order to provide the Services to a Customer Service Location, such Service Location must have Internet connectivity. The connectivity may be pre-existing or ordered in conjunction with the Services. Comcast supports the Services over Comcast EDI Service, Comcast Business Internet Service, or Internet connectivity services provided by a third-party service provider. If the underlying connectivity is terminated at a Service Location or unavailable for any reason at any time, the Services at said Service Location will be inoperable.

3. SD-WAN Services Technical Specifications

A. **Underlay connectivity.** This Service leverages the public Internet (Comcast on-net Layer 3 internet access services over fiber and DOCSIS, Comcast provided off-net Layer 3 internet access, or third-party-provided internet access, or LTE provided by Comcast or a third party).

B. **Hybrid WAN connectivity.** This Service will work over any industry standard third-party Layer 3 IP technology (*e.g.*, IP VPN and MPLS) which can serve as additional underlay to the public Internet.

C. **SD-WAN Overlay.** This Service uses Underlay Service access to establish IPSec VPN tunnels using AES-256 or AES-128 encryption between Comcast provided uCPEs as well as to provide control plane access from the uCPE to the SD-WAN controller. The SD-WAN software steers application traffic real time based on business policy rules provided by the Customer.

D. **SD-WAN uCPE.** Comcast will provide robust and flexible uCPEs. Such uCPEs are "x86" hardware that are service-agnostic and can host Comcast-provided applications.

E. **SD-WAN Firewall.** Comcast will provide a Layer 3/Layer 4 Stateful Firewall as part of this Service.

F. **Dynamic WAN utilization; Traffic Steering**. For Service Location-to-Service Location traffic, the Service automatically selects the best available WAN connection based on a combination of traffic flows and application policies that have been defined by Comcast and the Customer in the ACD. For Standalone, the Customer may prioritize certain applications and/or application groups to be re-routed in the event the primary route is unavailable, and to opt-in to LTE back-up on a per-application or per-application group basis; however, certain features of Dynamic WAN utilization are not available for Standalone.

G. **Service Orchestration.** Provisioning and configuration of connectivity, routing policies, security, and application aware traffic steering is provided through a centralized, geo-redundant orchestration plane that is logically segregated per Customer. Connectivity to the orchestration layer occurs through encrypted tunnels across the public Internet.

H. **Digital Experience.** Service visibility, control, and reporting is provided via the Comcast Business Digital Experience web portal ("**Portal**").

4. Optional SD-WAN Service Configurations

A. **Local Internet Breakout.** Comcast can configure a local Internet breakout at each Customer Service Location with the purpose of routing traffic directly to the Internet as needed. Local Internet breakout is not a connectivity service and is solely a route configuration inside the uCPE to allow local hosts to bypass the VPN tunnel and access the internet using the local underlay directly.

B. **High Availability**. High Availability is an optional price-impacting SD-WAN Service feature that enhances resiliency by eliminating the single point of failure at the hardware (uCPE) level. Two (2) uCPEs are placed at the Service Location, both connected to the network and functioning in Active/Active mode.

C. **IPSec Tunnels to Third Party Peers**. An optional SD-WAN Service feature that allows Customer to establish IPSec tunnels between Customer Systems and up to three (3) third-party peers' networks, applications, software-as-a-service solutions, or other business-to-business services not provided by Comcast ("**Third-Party System(s)**"), provided such Third-Party System supports policy-based VPN. Use of Third-Party Systems is subject to Customer's agreement with the relevant provider and not the Agreement. Further to the limitations of liability set forth in Section 5.1(C) of the General Terms and Conditions, Comcast does not control, and has no liability for, how Third-Party Systems or their providers use Customer's data or for any claim related to connecting Customer Systems to a Third-Party System via the Services, even where Comcast supports Customer in configuring IPSec tunnel(s). It is entirely within Comcast's discretion as to whether Comcast will provide support for IPSec tunnel configuration.

5. Service Delivery and Service Management

A. **Kick-off call**: Comcast will sponsor a kick-off call with the Customer to explain the Service delivery process and Comcast and Customer will review the Customer Expectations Document.

B. **Technical interview**: Comcast will engage Customer in one or more interviews related to Customer's network design initiatives. Comcast will document the technical information discovered through the interview process in an Architectural Confirmation Document and the Customer will review and confirm that the ACD is correct.

C. **Managed Install, Test, and Turn-up**: When Comcast installs the SD-WAN equipment, the configuration created for the Customer will be loaded onto the SD-WAN equipment and Comcast will test the Service.

D. **Network Monitoring and Management**: On and after the Service Commencement Date, Comcast will monitor the SD-WAN Service 24/7/365 and pull alarms from the equipment related to the availability of the Services. Comcast will send an alert to the Customer for specific, Service-impacting alarms. After receiving such an alarm, Comcast will open an internal ticket and begin to troubleshoot the issue.

E. **On-Going Solution Support**:

i. Configuration Changes. Comcast will support Customer-requested configuration changes, in accordance with Comcast's then current configuration change policy (the "**Configuration Change Policy**"). Upon request, Comcast shall provide Customer with its then current Configuration Change Policy. Any moves, additions, changes, or deletions to the Services shall be requested over the phone. This includes any changes to the Service configuration as initially outlined in the ACD. Comcast endeavors to meet the following configuration change response objectives:

STANDARD SD-WAN SERVICE	
Category	**Objective**
Simple Configuration Change	4 hours
Complex Configuration Change	48 hours

ADVANCED SD-WAN SERVICE	
Category	**Objective**
Simple Configuration Change	30 minutes
Complex Configuration Change	12 hours

"**Simple Configuration Change**" means changes such as firewall updates, traffic steering policies, quality of service changes, adding and removing IP addresses, and NAT and PAT changes.

"**Complex Configuration Change**" means changes such as WAN/LAN reconfiguration, DHCP scope changes, DNS changes, and changes to routing policies.

ii. Software Updates and Security Patches. If a Comcast vendor develops software updates and/or security patches for such vendor's equipment which Comcast uses to provide the Services, Comcast will upload such software updates and/or security patches to the applicable equipment to the extent Comcast determines, in its sole discretion, that such software updates and/or security patches are necessary. Updates or patches that are viewed as critical may require immediate action with a maintenance window. For the avoidance of doubt, Comcast shall have no obligation to develop software updates or security patches and its only obligation under this paragraph is to install updates and security patches developed by its applicable vendors to the extent Comcast determines, in its sole discretion, that such software updates and/or security patches are necessary.

iii. Technical Support. Comcast provides Customers a toll-free trouble reporting telephone number to reach the Enterprise Customer Care (ECC) that operates on a 24x7x365 basis. Comcast provides technical support for Service-related inquiries. Technical support will not offer consulting or advice on issues relating to non-Comcast Equipment.

iv. Escalation. Reported troubles are escalated within the Comcast Advanced Solutions Operations (AS Ops) to meet the standard restoration interval described in the Service Availability Objectives. For Service Interruptions (as defined in Schedule A-2), troubles are escalated within the Comcast AS Ops as follows: Supervisor at the end of the standard interval plus one (1) hour; to the Manager at the end of the standard interval plus two (2) hours, and to the Director at the end of the standard interval, plus four (4) hours.

v. Maintenance. Comcast's standard maintenance window is Sunday to Saturday from 12:00 a.m. to 6:00 a.m. local time. Scheduled maintenance is performed during the maintenance window and will be coordinated between Comcast and the Customer. Comcast provides a minimum of forty-eight (48) hours' notice for non-service impacting scheduled maintenance. Comcast provides a minimum of seven (7) days' notice for service impacting planned maintenance. Emergency maintenance is performed as needed.

6. Security Monitoring and Mitigation.

For the Services, Comcast monitors the equipment. **COMCAST DOES NOT PROVIDE MONITORING OF SECURITY EVENTS, ANY SECURITY EVENT MITIGATION, OR ADVICE REGARDING SECURITY ISSUES OR THREATS.** Upon request by Customer, Comcast will modify the configuration of the Services in accordance with specifications provided by Customer to attempt to mitigate security events and security threats identified by Customer. Comcast's sole obligation is to implement the configuration settings requested by Customer. This Service is provided on a commercially reasonable efforts basis only and Comcast makes no guarantees with respect to the detection or blocking of viruses/worm/malware or any other types of attacks and is not responsible for any such malicious data that may be transmitted over the provided network.

7. Customer Responsibilities

In addition to the responsibilities and obligations identified in the Customer Expectations Document, Customer shall have the following responsibilities related to the installation, support, and maintenance of the Service:

A. Provide an operating environment with temperatures not below fifty-five (55) or above eighty-five (85) degrees Fahrenheit. Humidity shall not exceed ninety (90) percent at eighty-five (85) degrees Fahrenheit.

B. Provide secure space sufficient for access to one (1) standard, freestanding equipment cabinet at each of the Customer facilities, no farther than fifty feet from the Customer router or switch interface.

C. Provide power including UPS AC power equipment, circuit sizing to be determined, if applicable.

D. Provide emergency local generator backup service, if applicable.

E. Provide access to the buildings and point of demarcation at each Customer Service Location to allow Comcast and its approved contractors to install uCPE. Provide access to each location for regular (8 a.m. - 5 p.m.) and emergency (24 hour) service and maintenance of Comcast's equipment and facilities.

F. If interfacing with a third-party IP service: provide, install and maintain a device that is capable of routing network traffic between the Service and the Customer's Wide Area Network (WAN).

G. Customer must provide a point of contact (POC) for installation, service activation, notices for Service Interruptions, and any maintenance activities.

H. Customer must approve the final Architecture Configuration Document (ACD) prior to installation of the Services.

I. Customer must ensure that any Customer-provided or existing Underlay Service is installed and operational prior to installation of the Services.

J. The demarcation point of the SD-WAN Service is the ActiveCore uCPE. Customer shall have sole responsibility for installing, configuring, providing and maintaining all customer LAN equipment.

K. With respect to IP SEC Tunnels to Third-Party Peers:

- Customer must provide all third-party technical information required for establishing IP Sec tunnel connectivity.
- Customer must establish and maintain all required accounts and infrastructure with the applicable third-party peer prior to any technical discussions with the ActiveCore Engineer or Solutions Architect.
- If Customer receives any infringement notices related to its use of Third-Party System(s), it must promptly: (a) stop using the related item with the Service; and (b) notify Comcast.

COMCAST ENTERPRISE SERVICES
PRODUCT-SPECIFIC ATTACHMENT
SD-WAN SERVICES

SCHEDULE A-2
SERVICE LEVEL AGREEMENTS AND OBJECTIVES

The Services are backed by the following Service Availability Objectives:

1. Definitions

Capitalized terms not otherwise defined herein shall have the meaning ascribed to them in the SD-WAN Services PSA or the General Terms and Conditions.

"Available" means the Service at a Service Location is available to transmit and receive data, as measured by Comcast's systems. The Service is considered "Available" whether data is passing through the primary connection or through a backup connection at a given Service Location.

"Planned Service Interruption" means any Service Interruption caused by planned work such as scheduled maintenance or planned enhancements or upgrades to the network.

"Service Interruption" means, subject to the exclusions set forth in Section 6 (Exceptions to Credit Allowance), the Service is completely Unavailable outside of Planned Service Interruption(s).

"Service Availability" means a percentage of time in a calendar month during which the Service is Available. The Service Availability percentage for a given calendar month is calculated as follows: (A/M) * 100, where A is the total number of minutes the Service was Available during such calendar month and M is the total number of minutes in such calendar month.

"Service Availability Objective(s)" means the intended Service Availability for a calendar month, as set forth in Section 2 below.

"**Unavailable**" means the Service is not Available (*i.e.*, the Service is completely unable to transmit or receive any data, as measured by Comcast's systems).

2. SD-WAN Service Level Agreement (SLA)

The Credit allowance available to Customer for failure to meet Service Availability Objectives shall be limited to the amounts set forth in the table below ("**Credits**"). For the purposes of calculating Credits for any such failure to meet a Service Availability Objective, (A) the Service Interruption on which such failure is based begins upon Comcast's creation of a trouble ticket for the earlier of: (i) an automatic Service Interruption alarm (as described in Section 5.D. of Schedule A-1), or (ii) Customer's report to Comcast of an interruption in the Service, provided that the interruption is reported by Customer during the duration of the interruption; and (B) the Service Interruption shall be deemed resolved upon closing of the same trouble ticket or, if sooner, the termination of the interruption, less any time Comcast is awaiting additional information or premises testing from the Customer. In no event shall the total amount of Credit issued to Customer's account on a per-month basis exceed fifty percent (50%) of the total monthly recurring charge ("**MRC**") associated with the impacted portion of the Service set forth in the Sales Order. Failures to meet Service Availability Objectives will not be aggregated for purposes of determining Credit allowances. To qualify, Customer must request the Credit from Comcast within thirty (30) days of the Service Interruption that resulted in failure to meet the Service Availability Objective. Customer will not be entitled to any additional credits for Service Interruptions or failures to meet the Service Availability Objective.

Service:	**Service Availability Objective:**	**Service Availability:**	**Amount of Credit:**
For Service Locations Not Configured as Standalone	99.99%	Equal to or greater than 99.99%	None
		Equal to or greater than 99.9% but less than 99.99%	5% of MRC

		Equal to or greater than 99% but less than 99.9%	10% of MRC
		Less than 99%	20% of MRC
For Service Locations Configured as Standalone	99.995%	Equal to or greater than 99.995%	None
		Equal to or greater than 99.9% but less than 99.995%	5% of MRC
		Equal to or greater than 99% but less than 99.9%	10% of MRC
		Less than 99%	20% of MRC

THE TOTAL CREDIT ALLOWANCE PER MONTH IS CAPPED AT FIFTY PERCENT (50%) OF THAT MONTH'S MRC FOR THE IMPACTED PORTIONS OF THE SERVICE. SEPARATELY OCCURRING SERVICE INTERRUPTIONS AND RESULTING FAILURES TO MEET SERVICE AVAILABILITY OBJECTIVES ARE NOT AGGREGATED FOR THE PURPOSES OF DETERMINING CREDIT ALLOWANCES.

3. Additional Service Availability Objectives

Comcast provides Service Availability Objectives for the Service, including mean time to respond, and mean time to restore. These service objectives are measured, on a calendar month basis, from the Comcast point of demarcation. Service availability is also affected by the choice of Underlay Service.

A. **Mean Time to Respond**. The Mean Time to Respond objective is the average time required for Comcast to begin troubleshooting a Service Interruption. The Mean Time to Respond objective is fifteen (15) minutes from the earlier of Comcast's receipt of a fault notification or from the time a trouble ticket is opened with Comcast.

B. **Mean Time to Restore**. The Mean Time to Restore objective is the average time required to restore Service after a Service Interruption to an operational condition as defined by the technical specifications in Section 1 of this Schedule. The Mean Time to Restore objective is as follows:

i. for Service Locations within the Comcast franchise footprint: Comcast will endeavor to restore the Service, including any required repair or replacement of uCPE, within four (4) hours of the time a customer reported trouble ticket is opened with Comcast.

ii. for Service Locations outside the Comcast franchise footprint: Comcast will endeavor to restore the Service, including any required repair or replacement of uCPE, the next Business Day after the day on which a customer reported trouble ticket is opened with Comcast; provided the trouble ticket is opened before 1:00 p.m. EST on a Business Day. For trouble tickets opened on Saturday, Sunday, a holiday, or after 1:00 p.m. EST on a Business Day, Comcast will endeavor to restore the Service the second Business Day thereafter. "Business Days" are Monday through Friday, excluding federal holidays.

4. Emergency Blocking

The parties agree that if either party hereto, in its reasonable sole discretion, determines that an emergency action is necessary to protect its own network, the party may, after engaging in reasonable and good faith efforts to notify the other party of the need to block, block any transmission path over its network by the other party where transmissions do not meet material standard industry requirements. The parties further agree that none of their respective obligations to one another under the Agreement will be affected by any such blockage except that the party affected by such blockage will be relieved of all obligations to make payments for charges relating to the circuit(s) which is so blocked and that no party will have any obligation to the other party for any claim, judgment, or liability resulting from such blockage.

5. Remedy Processes

All claims and rights arising under this Service Level Agreement must be exercised by Customer in writing within thirty (30) days of the event that gave rise to the claim or right. The Customer must submit the following information to the Customer's Comcast account representative with any and all claims for Credit allowances: (a) organization name; (b) Customer account number; and (c) basis of

Credit allowance claim (including date and time, if applicable). Comcast will acknowledge and review all claims promptly and will inform the Customer by electronic mail or other correspondence whether a Credit allowance will be issued or the claim rejected, with the reasons specified for the rejection.

6. Exceptions to Credit Allowances

Comcast shall not be liable for any Service Interruption, and a Service Interruption shall not qualify for the remedies set forth herein, if such Service Interruption is related to, associated with, or caused by: force majeure events, Planned Service Interruptions, Customer actions or inactions; Customer-Provided Equipment or power; or any third party not contracted through Comcast, including, without limitation, Customer's users, third-party network providers, any power, equipment or services provided by third parties.

7. Eligibility for Credit Allowances

In order to be eligible for Credits, each Service Location must have at least two primary WAN interfaces from at least two Underlay Service providers.

8. Other Limitations

The remedies set forth in this Service Level Agreement shall be Customer's sole and exclusive remedies for any Service Interruption, outage, unavailability, delay, or other degradation, or any Comcast failure to meet the Service Availability Objectives.

SCHEDULE A-3
RESPONSIBILITY MATRIX

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
1	***Requirement 1: Install and maintain a firewall configuration to protect cardholder data***		
1.1	**1.1** Establish and implement firewall and router configuration standards that include the following:	Shared	Comcast is responsible for configuration standards for the uCPE and backend system components. Customer is responsible for configuration standards for the components in its CDE and components that connect to the uCPE.
1.1.1	**1.1.1** A formal process for approving and testing all network connections and changes to the firewall and router configurations	Shared	Comcast is responsible for configuration standards for the uCPE and backend system components. Customer is responsible for configuration standards for the components in its CDE and components that connect to the uCPE.
1.1.2	**1.1.2** Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	Shared	Comcast is responsible for configuration standards for the uCPE and backend system components. Customer is responsible for configuration standards for the components in its CDE and components that connect to the uCPE.
1.1.3	**1.1.3** Current diagram that shows all cardholder data flows across systems and networks	Customer	Though configuration standards are a shared responsibility, Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
1.1.4	**1.1.4** Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	Shared	Comcast is responsible for configuration standards for the uCPE and backend system components. Customer is responsible for configuration standards for the components in its CDE and components that connect to the uCPE.
1.1.5	**1.1.5** Description of groups, roles, and responsibilities for management of network components	Shared	Comcast is responsible for configuration standards for the uCPE and backend system components. Customer is responsible for configuration standards for the components in its CDE and components that connect to the uCPE.
1.1.6	**1.1.6** Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	Shared	Comcast is responsible for configuration standards for the uCPE and backend system components. Customer is responsible for configuration standards for the components in its CDE and components that connect to the uCPE.
1.1.7	**1.1.7** Requirement to review firewall and router rule sets at least every six months	Shared	Comcast is responsible for configuration standards for the uCPE and backend system components. Customer is responsible for configuration standards for the components in its CDE and components that connect to the uCPE.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
1.2	**1.2** Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. ***Note:*** *An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*	Shared	Comcast is responsible for building configurations that restrict connections between untrusted networks and its backend system components. Customer is responsible for building configurations that restrict connections between untrusted networks and the uCPE and its CDE.
1.2.1	**1.2.1** Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	Shared	Comcast is responsible for building configurations that restrict connections between untrusted networks and its backend system components. Customer is responsible for building configurations that restrict connections between untrusted networks and the uCPE and its CDE.
1.2.2	**1.2.2** Secure and synchronize router configuration files.	Shared	Comcast is responsible for building configurations that restrict connections between untrusted networks and its backend system components. Customer is responsible for building configurations that restrict connections between untrusted networks and the uCPE and its CDE.
1.2.3	**1.2.3** Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	Shared	Comcast is responsible for building configurations that restrict connections between untrusted networks and its backend system components. Customer is responsible for building configurations that restrict connections between untrusted networks and the uCPE and its CDE.
1.3	**1.3** Prohibit direct public access between the Internet and any system component in the cardholder data environment**.**	Shared	Comcast is responsible for prohibiting direct public access between the Internet and its backend system components. Customer is responsible for prohibiting direct public access between the Internet and the uCPE and its CDE.
1.3.1	**1.3.1** Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	Shared	Comcast is responsible for prohibiting direct public access between the Internet and its backend system components. Customer is responsible for prohibiting direct public access between the Internet and the uCPE and its CDE.
1.3.2	**1.3.2** Limit inbound Internet traffic to IP addresses within the DMZ.	Shared	Comcast is responsible for prohibiting direct public access between the Internet and its backend system components. Customer is responsible for prohibiting direct public access between the Internet and the uCPE and its CDE.
1.3.3	**1.3.3** Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)	Shared	Comcast is responsible for prohibiting direct public access between the Internet and its backend system components. Customer is responsible for prohibiting direct public access between the Internet and the uCPE and its CDE.
1.3.4	**1.3.4** Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	Shared	Comcast is responsible for prohibiting direct public access between the Internet and its backend system components. Customer is responsible for prohibiting direct public access between the Internet and the uCPE and its CDE.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
1.3.5	**1.3.5** Permit only "established" connections into the network.	Shared	Comcast is responsible for prohibiting direct public access between the Internet and its backend system components. Customer is responsible for prohibiting direct public access between the Internet and the uCPE and its CDE.
1.3.6	**1.3.6** Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	Customer	Though prohibiting direct public access from the Internet is a shared responsibility, Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
1.3.7	**1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties.** **Note:** Methods to obscure IP addressing may include, but are not limited to: · Network Address Translation (NAT) · Placing servers containing cardholder data behind proxy servers/firewalls, · Removal or filtering of route advertisements for private networks that employ registered addressing, · Internal use of RFC1918 address space instead of registered addresses.	Shared	Comcast is responsible for prohibiting direct public access between the Internet and its backend system components. Customer is responsible for prohibiting direct public access between the Internet and the uCPE and its CDE.
1.4	**1.4** Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include: · Specific configuration settings are defined. · Personal firewall (or equivalent functionality) is actively running. · Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.	Shared	Comcast is responsible for installing personal firewall software or equivalent functionality on any portable computing devices that connects to the Internet when outside the network, and which are also used to access the uCPE and backend system components. Customer is responsible for installing personal firewall software or equivalent functionality on any portable computing devices that connect to the Internet when outside the network, and which are also used to access the uCPE and its CDE.
1.5	**1.5** Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.	Shared	Comcast is responsible for security policies and operational procedures for managing the uCPE and backend system components. Customer is responsible for security policies and operational procedures for managing components in its CDE and components that connect to the uCPE.
2	***Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters***		
2.1	**2.1** Always change vendor-supplied defaults and remove or disable unnecessary default accounts **before** installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, *point-of-sale (*POS*)* terminals, Simple Network Management Protocol (SNMP) community strings, etc.).	Shared	Comcast is responsible for changing vendor-supplied defaults and removing or disabling unnecessary default accounts on the uCPE and backend system components. Customer is responsible for changing vendor-supplied defaults and removing or disabling unnecessary default accounts on components in its CDE and on components that connect to the uCPE.

Req.	PCI DSS v3.2.1 Requirements		Responsibility (Comcast / Customer / Shared)	Responsibility Summary
2.1.1		**2.1.1** For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	Customer	Though changing and/or removing defaults is a shared responsibility, Comcast does not deploy a wireless environment as part of the SD-WAN product, so this requirement is the sole responsibility of the customer.
2.2		**2.2** Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: · Center for Internet Security (CIS) · International Organization for Standardization (ISO) · SysAdmin Audit Network Security (SANS) Institute · National Institute of Standards Technology (NIST).	Shared	Comcast is responsible for configuration standards for the uCPE and backend system components. Customer is responsible for configuration standards for the components in its CDE and components that connect to the uCPE.
2.2.1		**2.2.1** Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) ***Note:*** *Where virtualization technologies are in use, implement only one primary function per virtual system component.*	Shared	Comcast is responsible for configuration standards for the uCPE and backend system components. Customer is responsible for configuration standards for the components in its CDE and components that connect to the uCPE.
2.2.2		**2.2.2** Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	Shared	Comcast is responsible for configuration standards for the uCPE and backend system components. Customer is responsible for configuration standards for the components in its CDE and components that connect to the uCPE.
2.2.3		**2.2.3** Implement additional security features for any required services, protocols, or daemons that are considered to be insecure. **Note:** Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.	Shared	Comcast is responsible for configuration standards for the uCPE and backend system components. Customer is responsible for configuration standards for the components in its CDE and components that connect to the uCPE.
2.2.4		**2.2.4** Configure system security parameters to prevent misuse.	Shared	Comcast is responsible for configuration standards for the uCPE and backend system components.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
			Customer is responsible for configuration standards for the components in its CDE and components that connect to the uCPE.
2.2.5	**2.2.5** Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	Shared	Comcast is responsible for configuration standards for the uCPE and backend system components. Customer is responsible for configuration standards for the components in its CDE and components that connect to the uCPE.
2.3	**2.3** Encrypt all non-console administrative access using strong cryptography.	Shared	Comcast is responsible for encrypting all non-console administrative access to the uCPE and backend system components. Customer is responsible for encrypting all non-console administrative access to components in its CDE and components that connect to the uCPE.
2.4	**2.4** Maintain an inventory of system components that are in scope for PCI DSS.	Shared	Comcast is responsible for maintaining an inventory of the uCPEs and backend system components. Customer is responsible for maintaining an inventory of components in its CDE and components that connect to the uCPE.
2.5	**2.5** Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	Shared	Comcast is responsible for security policies and operational procedures for managing the uCPE and backend system components. Customer is responsible for security policies and operational procedures for managing components in its CDE and components that connect to the uCPE.
2.6	**2.6** Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers.	N/A	
3	***Requirement 3: Protect stored cardholder data***		
3.1	**3.1** Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
	· Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements · Specific retention requirements for cardholder data · Processes for secure deletion of data when no longer needed · A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.		
3.2	**3.2** Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. *It is permissible for issuers and companies that support issuing services to store sensitive authentication data if:* · There is a business justification and · The data is stored securely. Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.2.1	**3.2.1** Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. ***Note:*** *In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* · *The cardholder's name* · *Primary account number (PAN)* · *Expiration date* · *Service code* *To minimize risk, store only these data elements as needed for business.*	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.2.2	**3.2.2** Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card- not-present transactions after authorization.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.2.3	**3.2.3** Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.3	**3.3** Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
	legitimate business need can see more than the first six/last four digits of the PAN. **Note:** This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.		
3.4	**3.4** Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: · One-way hashes based on strong cryptography, (hash must be of the entire PAN) · Truncation (hashing cannot be used to replace the truncated segment of PAN) · Index tokens and pads (pads must be securely stored) · Strong cryptography with associated key-management processes and procedures. ***Note:*** *It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.*	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.4.1	**3.4.1** If disk encryption is used (rather than file-or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts. **Note:** This requirement applies in addition to all other PCI DSS encryption and key-management requirements.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.5	**3.5** Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse: ***Note:*** *This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys— such key-encrypting keys must be at least as strong as the data-encrypting key.*	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
3.5.1	**3.5.1** Additional requirement for service providers only: Maintain a documented description of the cryptographic architecture that includes: · Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date · Description of the key usage for each key · Inventory of any HSMs and other SCDs used for key management Note:	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.5.2	**3.5.2** Restrict access to cryptographic keys to the fewest number of custodians necessary.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.5.3	**3.5.3** Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: · Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key · Within a secure cryptographic device (such as a host security module (HSM) or PTS-approved point-of-interaction device) · As at least two full-length key components or key shares, in accordance with an industry-accepted method ***Note:*** *It is not required that public keys be stored in one of these forms.*	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.5.4	**3.5.4** Store cryptographic keys in the fewest possible locations.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.6	**3.6** Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: ***Note:*** *Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.*	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.6.1	**3.6.1** Generation of strong cryptographic keys	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.6.2	**3.6.2** Secure cryptographic key distribution	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.6.3	**3.6.3** Secure cryptographic key storage	Customer	

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
			Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.6.4	**3.6.4** Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher- text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.6.5	**3.6.5** Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised. ***Note:*** *If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.*	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.6.6	**3.6.6** If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control. ***Note:*** *Examples of manual key- management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.*	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.6.7	**3.6.7** Prevention of unauthorized substitution of cryptographic keys.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.6.8	**3.6.8** Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.7	**3.7** Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
4	***Requirement 4: Encrypt transmission of cardholder data across open, public networks***		
4.1	**4.1** Use strong cryptography and security protocols to safeguard sensitive cardholder data during	Customer	

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
	transmission over open, public networks, including the following: · Only trusted keys and certificates are accepted. · The protocol in use only supports secure versions or configurations. · The encryption strength is appropriate for the encryption methodology in use. **Note:** Where SSL/early TLS is used, the requirements in Appendix A2 must be completed. Examples of open, public networks include but are not limited to: · The Internet · Wireless technologies, including 802.11 and Bluetooth · Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA) · General Packet Radio Service (GPRS) · Satellite communications		Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
4.1.1	**4.1.1** Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
4.2	**4.2** Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
4.3	**4.3** Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
5	***Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs***		
5.1	**5.1** Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	Shared	Comcast is responsible for deploying anti-virus software on backend system components that are commonly affected by malicious software. Customer is responsible for deploying anti-virus software on components in its CDE and on components that connect to the uCPE.
5.1.1	**5.1.1** Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	Shared	Comcast is responsible for deploying anti-virus software on backend system components that are commonly affected by malicious software. Customer is responsible for deploying anti-virus software on components in its CDE and on components that connect to the uCPE.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
5.1.2	**5.1.2** For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.	Shared	Comcast is responsible for deploying anti-virus software on backend system components that are commonly affected by malicious software. Customer is responsible for deploying anti-virus software on components in its CDE and on components that connect to the uCPE.
5.2	**5.2** Ensure that all anti-virus mechanisms are maintained as follows: · Are kept current, · Perform periodic scans · Generate audit logs which are retained per PCI DSS Requirement 10.7.	Shared	Comcast is responsible for maintaining anti-virus software on backend system components that are commonly affected by malicious software. Customer is responsible for maintaining anti-virus software on components in its CDE and on components that connect to the the uCPE.
5.3	**5.3** Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. ***Note:*** *Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.*	Shared	Comcast is responsible for maintaining anti-virus software on backend system components that are commonly affected by malicious software. Customer is responsible for maintaining anti-virus software on components in its CDE and those that connect to the the uCPE.
5.4	**5.4** Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	Shared	Comcast is responsible for security policies and operational procedures for protecting backend system components. Customer is responsible for security policies and operational procedures for protecting components in its CDE and components that connect to the uCPE.
6	***Requirement 6: Develop and maintain secure systems and applications***		
6.1	**6.1** Establish a process to identify security vulnerabilities, using reputable outside sources for	Shared	

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
	security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities. ***Note:*** *Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected.* *Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk- assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.*		Comcast is responsible for establishing a process to identify security vulnerabilities affecting the uCPE and backend system components. Customer is responsible for establishing a process to identify security vulnerabilities affecting components in its CDE and components that connect to the uCPE.
6.2	**6.2** Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor- supplied security patches. Install critical security patches within one month of release. ***Note:*** *Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.*	Shared	Comcast is responsible for installing applicable vendor-supplied security patches on the uCPE and backend system components. Customer is responsible for installing patches on components in its CDE and on components that connect to the uCPE.
6.3	**6.3** Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: · In accordance with PCI DSS (for example, secure authentication and logging) · Based on industry standards and/or best practices. · Incorporating information security throughout the software-development life cycle Note: this applies to all software developed internally as well as bespoke or custom software developed by a third party.	Shared	Comcast is responsible for developing secure software for those applications deployed to the uCPE and backend system components based on industry standards and/or best practices. Customer is responsible for developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.
6.3.1	**6.3.1** Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	Shared	Comcast is responsible for developing secure software for those applications deployed to the uCPE and backend system components based on industry standards and/or best practices. Customer is responsible for developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.
6.3.2	**6.3.2** Review custom code prior to release to production or customers in order to identify	Shared	

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
	any potential coding vulnerability (using either manual or automated processes) to include at least the following: · Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices. · Code reviews ensure code is developed according to secure coding guidelines · Appropriate corrections are implemented prior to release. · Code-review results are reviewed and approved by management prior to release. *Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle.* *Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.*		Comcast is responsible for developing secure software for those applications deployed to the uCPE and backend system components based on industry standards and/or best practices. Customer is responsible for developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.
6.4	**6.4** Follow change control processes and procedures for all changes to system components. The processes must include the following:	Shared	Comcast is responsible for following control processes and procedures for changes to the uCPE operating system and backend system components. Customer is responsible for following control processes and procedures for changes to the uCPE it makes via the Activecore Portal, to components in its CDE, and to components connected to the uCPE.
6.4.1	**6.4.1** Separate development/test environments from production environments, and enforce the separation with access controls.	Shared	Comcast is responsible for following control processes and procedures for changes to the uCPE operating system and backend system components. Customer is responsible for following control processes and procedures for changes to the uCPE it makes via the Activecore Portal, to components in its CDE, and to components connected to the uCPE.
6.4.2	**6.4.2** Separation of duties between development/test and production environments	Shared	Comcast is responsible for following control processes and procedures for changes to the uCPE operating system and backend system components. Customer is responsible for following control processes and procedures for changes to the uCPE it makes via the Activecore Portal, to components in its CDE, and to components connected to the uCPE.
6.4.3	**6.4.3** Production data (live PANs) are not used for testing or development	Shared	

Req.	PCI DSS v3.2.1 Requirements		Responsibility (Comcast / Customer / Shared)	Responsibility Summary
				Comcast is responsible for following control processes and procedures for changes to the uCPE operating system and backend system components. Customer is responsible for following control processes and procedures for changes to the uCPE it makes via the Activecore Portal, to components in its CDE, and to components connected to the uCPE.
6.4.4		**6.4.4** Removal of test data and accounts from system components before the system becomes active / goes into production.	Shared	Comcast is responsible for following control processes and procedures for changes to the uCPE operating system and backend system components. Customer is responsible for following control processes and procedures for changes to the uCPE it makes via the Activecore Portal, to components in its CDE, and to components connected to the uCPE.
6.4.5		**6.4.5** Change control procedures for the implementation of security patches and software modifications must include the following:	Shared	Comcast is responsible for following control processes and procedures for changes to the uCPE operating system and backend system components. Customer is responsible for following control processes and procedures for changes to the uCPE it makes via the Activecore Portal, to components in its CDE, and to components connected to the uCPE.
6.4.5.1		**6.4.5.1** Documentation of impact.	Shared	Comcast is responsible for following control processes and procedures for changes to the uCPE operating system and backend system components. Customer is responsible for following control processes and procedures for changes to the uCPE it makes via the Activecore Portal, to components in its CDE, and to components connected to the uCPE.
6.4.5.2		**6.4.5.2** Documented change approval by authorized parties.	Shared	Comcast is responsible for following control processes and procedures for changes to the uCPE operating system and backend system components. Customer is responsible for following control processes and procedures for changes to the uCPE it makes via the Activecore Portal, to components in its CDE, and to components connected to the uCPE.
6.4.5.3		**6.4.5.3** Functionality testing to verify that the change does not adversely impact the security of the system.	Shared	Comcast is responsible for following control processes and procedures for changes to the uCPE operating system and backend system components. Customer is responsible for following control processes and procedures for changes to the uCPE it makes via the Activecore Portal, to components in its CDE, and to components connected to the uCPE.
6.4.5.4		**6.4.5.4** Back-out procedures.	Shared	Comcast is responsible for following control processes and procedures for changes to the uCPE operating system and backend system components. Customer is responsible for following control processes and procedures for changes to the uCPE it makes via the Activecore Portal, to components in its CDE, and to components connected to the uCPE.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
	6.4.6 Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.	Shared	Comcast is responsible for following control processes and procedures for changes to the uCPE operating system and backend system components. Customer is responsible for following control processes and procedures for changes to the uCPE it makes via the Activecore Portal, to components in its CDE, and to components connected to the uCPE.
6.5	**6.5** Address common coding vulnerabilities in software-development processes as follows: · Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities. · Develop applications based on secure coding guidelines. **Note:** The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.	Shared	Comcast is responsible for training developers and developing software securely for those applications deployed to the uCPE and backend system components. Customer is responsible for training developers and developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.
6.5.1	**6.5.1** Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	Shared	Comcast is responsible for training developers and developing software securely for those applications deployed to the uCPE and backend system components. Customer is responsible for training developers and developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.
6.5.2	**6.5.2** Buffer overflows	Shared	Comcast is responsible for training developers and developing software securely for those applications deployed to the uCPE and backend system components. Customer is responsible for training developers and developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.
6.5.3	**6.5.3** Insecure cryptographic storage	Shared	Comcast is responsible for training developers and developing software securely for those applications deployed to the uCPE and backend system components. Customer is responsible for training developers and developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.
6.5.4	**6.5.4** Insecure communications	Shared	Comcast is responsible for training developers and developing software securely for those applications deployed to the uCPE and backend system components. Customer is responsible for training developers and developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.

Req.	PCI DSS v3.2.1 Requirements		Responsibility (Comcast / Customer / Shared)	Responsibility Summary
6.5.5		**6.5.5** Improper error handling	Shared	Comcast is responsible for training developers and developing software securely for those applications deployed to the uCPE and backend system components. Customer is responsible for training developers and developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.
6.5.6		**6.5.6** All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).	Shared	Comcast is responsible for training developers and developing software securely for those applications deployed to the uCPE and backend system components. Customer is responsible for training developers and developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.
		Note: Requirements 6.5.7 through 6.5.10, below, apply to web applications and application interfaces (internal or external):		
6.5.7		**6.5.7** Cross-site scripting (XSS)	Shared	Comcast is responsible for training developers and developing software securely for those applications deployed to the uCPE and backend system components. Customer is responsible for training developers and developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.
6.5.8		**6.5.8** Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).	Shared	Comcast is responsible for training developers and developing software securely for those applications deployed to the uCPE and backend system components. Customer is responsible for training developers and developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.
6.5.9		**6.5.9** Cross-site request forgery (CSRF)	Shared	Comcast is responsible for training developers and developing software securely for those applications deployed to the uCPE and backend system components. Customer is responsible for training developers and developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.
6.5.10		**6.5.10** Broken authentication and session management	Shared	Comcast is responsible for training developers and developing software securely for those applications deployed to the uCPE and backend system components. Customer is responsible for training developers and developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
6.6	**6.6** For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: · Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes ***Note:*** *This assessment is not the same as the vulnerability scans performed for Requirement 11.2.* · Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.	Shared	Comcast is responsible for addressing new threats and vulnerabilities applicable to public-facing web applications hosted on backend system components. Customer is responsible for addressing new threats and vulnerabilities applicable to public-facing web applications hosted in its CDE.
6.7	**6.7** Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.	Shared	Comcast is responsible for security policies and operational procedures for developing and maintaining secure systems and applications deployed to the uCPE and backend system components. Customer is responsible for security policies and operational procedures for developing and maintaining secure systems and applications deployed to components in its CDE and to components that connect to the uCPE.
7	***Requirement 7: Restrict access to cardholder data by business need to know***		
7.1	**7.1** Limit access to system components and cardholder data to only those individuals whose job requires such access.	Shared	Comcast is responsible for limiting access to the uCPE (via underlying operating system) and backend system components. Customer is responsible for limiting access to the uCPE (via Activecore Portal), to components in its CDE, and to components that connect to the uCPE.
7.1.1	**7.1.1** Define access needs for each role, including: · System components and data resources that each role needs to access for their job function · Level of privilege required (for example, user, administrator, etc.) for accessing resources.	Shared	Comcast is responsible for limiting access to the uCPE (via underlying operating system) and backend system components. Customer is responsible for limiting access to the uCPE (via Activecore Portal), to components in its CDE, and to components that connect to the uCPE.
7.1.2	**7.1.2** Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	Shared	Comcast is responsible for limiting access to the uCPE (via underlying operating system) and backend system components. Customer is responsible for limiting access to the uCPE (via Activecore Portal), to components in its CDE, and to components that connect to the uCPE.
7.1.3	**7.1.3** Assign access based on individual personnel's job classification and function.	Shared	Comcast is responsible for limiting access to the uCPE (via underlying operating system) and backend system components. Customer is responsible for limiting access to the uCPE (via Activecore Portal), to components in its CDE, and to components that connect to the uCPE.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
7.1.4	**7.1.4** Require documented approval by authorized parties specifying required privileges.	Shared	Comcast is responsible for limiting access to the uCPE (via underlying operating system) and backend system components. Customer is responsible for limiting access to the uCPE (via Activecore Portal), to components in its CDE, and to components that connect to the uCPE.
7.2	**7.2** Establish an access control system for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:	Shared	Comcast is responsible for restricting access to the uCPE (via underlying operating system) and backend system components. Customer is responsible for restricting access to the uCPE (via Activecore Portal), to components in its CDE, and to components that connect to the uCPE.
7.2.1	**7.2.1** Coverage of all system components	Shared	Comcast is responsible for restricting access to the uCPE (via underlying operating system) and backend system components. Customer is responsible for restricting access to the uCPE (via Activecore Portal), to components in its CDE, and to components that connect to the uCPE.
7.2.2	**7.2.2** Assignment of privileges to individuals based on job classification and function.	Shared	Comcast is responsible for restricting access to the uCPE (via underlying operating system) and backend system components. Customer is responsible for restricting access to the uCPE (via Activecore Portal), to components in its CDE, and to components that connect to the uCPE.
7.2.3	**7.2.3** Default "deny-all" setting.	Shared	Comcast is responsible for restricting access to the uCPE (via underlying operating system) and backend system components. Customer is responsible for restricting access to the uCPE (via Activecore Portal), to components in its CDE, and to components that connect to the uCPE.
7.3	**7.3** Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.	Shared	Comcast is responsible for security policies and operational procedures for restricting access to the uCPE (via underlying operating system) and backend system components. Customer is responsible for security policies and operational procedures for restricting access to the uCPE (via Activecore Portal), to components in its CDE, and to components that connect to the uCPE.
8	***Requirement 8: Identify and authenticate access to system components***		
8.1	**8.1** Define and implement policies and procedures to ensure proper user identification management for non- consumer users and administrators on all system components as follows:	Shared	Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components. Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.
8.1.1	**8.1.1** Assign all users a unique ID before allowing them to access system components or cardholder data.	Shared	Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components. Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
8.1.2	**8.1.2** Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	Shared	Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components. Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.
8.1.3	**8.1.3** Immediately revoke access for any terminated users.	Shared	Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components. Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.
8.1.4	**8.1.4** Remove/disable inactive user accounts at least every 90 days.	Shared	Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components. Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.
8.1.5	**8.1.5** Manage IDs used by third parties to access, support, or maintain system components via remote access as follows: · Enabled only during the time period needed and disabled when not in use. · Monitored when in use.	Customer	Comcast does not allow third parties to access in-scope systems. All access,if needed, is done through screen shares and is monitored at all times. For third-party access to customer systems which connect to the uCPE, this requirement is the sole responsibility of the customer.
8.1.6	**8.1.6** Limit repeated access attempts by locking out the user ID after not more than six attempts.	Shared	Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components. Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.
8.1.7	**8.1.7** Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	Shared	Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components. Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.
8.1.8	**8.1.8** If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	Shared	Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components. Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
8.2	**8.2** In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: · Something you know, such as a password or passphrase · Something you have, such as a token device or smart card · Something you are, such as a biometric.	Shared	Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components. Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.
8.2.1	**8.2.1** Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	Shared	Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components. Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.
8.2.2	**8.2.2** Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.	Shared	Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components. Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.
8.2.3	**8.2.3** Passwords/phrases must meet the following: · Require a minimum length of at least seven characters. · Contain both numeric and alphabetic characters. Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.	Shared	Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components. Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.
8.2.4	**8.2.4** Change user passwords/passphrases at least every 90 days.	Shared	Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components. Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.
8.2.5	**8.2.5** Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.	Shared	Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components. Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
8.2.6	**8.2.6** Set passwords/phrases for first- time use and upon reset to a unique value for each user, and change immediately after the first use.	Shared	Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components. Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.
8.3	**8.3** Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication. **Note:** Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.	Shared	Comcast is responsible for securing all individual non-console administrative access and all remote access using multi-factor authentication to the uCPE and backend system components. Customer is responsible for securing all individual non-console administrative access and all remote access using multi-factor authentication to components in its CDE and to components that connect to the uCPE.
8.3.1	**8.3.1** Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	Shared	Comcast is responsible for securing all individual non-console administrative access and all remote access using multi-factor authentication to the uCPE and backend system components. Customer is responsible for securing all individual non-console administrative access and all remote access using multi-factor authentication to components in its CDE and to components that connect to the uCPE.
8.3.2	**8.3.2** Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network.	Shared	Comcast is responsible for securing all individual non-console administrative access and all remote access using multi-factor authentication to the uCPE and backend system components. Customer is responsible for securing all individual non-console administrative access and all remote access using multi-factor authentication to components in its CDE and to components that connect to the uCPE.
8.4	**8.4** Document and communicate authentication procedures and policies to all users including: · Guidance on selecting strong authentication credentials · Guidance for how users should protect their authentication credentials · Instructions not to reuse previously used passwords · Instructions to change passwords if there is any suspicion the password could be compromised.	Shared	Comcast is responsible for documenting and communication authentication procedures and policies to users on the uCPE (via underlying operating systems) and backend system components. Customer is responsible for securing all individual non-console administrative access and all remote access using multi-factor authentication to components in its CDE and to components that connect to the uCPE.
8.5	**8.5** Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: · Generic user IDs are disabled or removed. · Shared user IDs do not exist for system administration and other critical functions. · Shared and generic user IDs are not used to administer any system components.	Shared	Comcast is responsible for not using group, shared, or generic IDs, passwords, or other authentication methods for the uCPE (via underlying operating systems) and backend system components. Customer is responsible for not using group, shared, or generic IDs, passwords, or other authentication methods for components in its CDE and for components that connect to the uCPE.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
8.5.1	**8.5.1** ***Additional requirement for service providers:*** Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer. ***Note:*** *This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.*	Comcast	
8.6	**8.6** Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: · Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. · Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.	Shared	Comcast is responsible for authentication methods for the uCPE and backend system components. Customer is responsible for authentication methods for components in its CDE and for components that connect to the uCPE.
8.7	**8.7** All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: · All user access to, user queries of, and user actions on databases are through programmatic methods. · Only database administrators have the ability to directly access or query databases. · Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
8.8	**8.8** Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.	Shared	Comcast is responsible for security policies and operational procedures for identification and authentication for the uCPE and backend system components. Customer is responsible for security policies and operational procedures for identification and authentication for components in its CDE, and for components that connect to the uCPE.
9	***Requirement 9: Restrict physical access to cardholder data***		
9.1	**9.1** Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.1.1	**9.1.1** Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
	least three months, unless otherwise restricted by law. ***Note:*** *"Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of- sale terminals are present, such as the cashier areas in a retail store.*		
9.1.2	**9.1.2** Implement physical and/or logical controls to restrict access to publicly accessible network jacks. *For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.*	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.1.3	**9.1.3** Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.2	**9.2** Develop procedures to easily distinguish between onsite personnel and visitors, to include: · Identifying new onsite personnel or visitors (for example, assigning badges) · Changes to access requirements · Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).	Shared	Comcast is responsible for procedures for distinguishing between onsite personnel and visitors on its property. Customer is responsible for procedures for distinguishing between onsite personnel and visitors on its property.
9.3	**9.3** Control physical access for onsite personnel to the sensitive areas as follows: · Access must be authorized and based on individual job function. · Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.4	**9.4** Implement procedures to identify and authorize visitors. Procedures should include the following:	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.4.1	**9.4.1** Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.4.2	**9.4.2** Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
9.4.3	**9.4.3** Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.4.4	**9.4.4** A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.5	**9.5** Physically secure all media.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.5.1	**9.5.1** Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.6	**9.6** Maintain strict control over the internal or external distribution of any kind of media, including the following:	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.6.1	**9.6.1** Classify media so the sensitivity of the data can be determined.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.6.2	**9.6.2** Send the media by secured courier or other delivery method that can be accurately tracked.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.6.3	**9.6.3** Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.7	**9.7** Maintain strict control over the storage and accessibility of media.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.7.1	**9.7.1** Properly maintain inventory logs of all media and conduct media inventories at least annually.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.8	**9.8** Destroy media when it is no longer needed for business or legal reasons as follows:	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.8.1	**9.8.1** Shred, incinerate, or pulp hard- copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
9.8.2	**9.8.2** Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.9	**9.9** Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. ***Note:*** *These requirements apply to card- reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.*	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.9.1	**9.9.1** Maintain an up-to-date list of devices. The list should include the following: · Make, model of device · Location of device (for example, the address of the site or facility where the device is located) · Device serial number or other method of unique identification.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.9.2	**9.9.2** Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). ***Note:*** *Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.*	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.9.3	**9.9.3** Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: · Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. · Do not install, replace, or return devices without verification. · Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). · Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
9.10	**9.10** Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.	Shared	Comcast is reponsible for security policies and operational procedures for restricting physical access to systems at Comcast owned locations. Customer is responsible for security policies and operational procedures for restricting physical access to systems at its locations.
10	***Requirement 10: Track and monitor all access to network resources and cardholder data***		
10.1	**10.1** Implement audit trails to link all access to system components to each individual user.	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.2	**10.2** Implement automated audit trails for all system components to reconstruct the following events:	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.2.1	**10.2.1** All individual user accesses to cardholder data	Customer	Though implementing audit trails is a shared responsibility, Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
10.2.2	**10.2.2** All actions taken by any individual with root or administrative privileges	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.2.3	**10.2.3** Access to all audit trails	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.2.4	**10.2.3** Access to all audit trails	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.2.5	**10.2 5** Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.2.6	**10.2.6** Initialization, stopping, or pausing of the audit logs	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.2.7	**10.2.7** Creation and deletion of system- level objects	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
10.3	**10.3** Record at least the following audit trail entries for all system components for each event:		Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.3.1	**10.3.1** User identification	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.3.2	**10.3.2** Type of event	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.3.3	**10.3.3** Date and time	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.3.4	**10.3.4** Success or failure indication	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.3.5	**10.3.5** Origination of event	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.3.6	**10.3.6** Identity or name of affected data, system component, or resource.	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.4	**10.4** Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. ***Note:*** *One example of time synchronization technology is Network Time Protocol (NTP).*	Shared	Comcast is responsible for using time-synchronization technology to synchornize clocks on the uCPE and backend system components. Customer is responsible for using time-synchronization technology to synchornize clocks on components in its CDE and on components connected to the uCPE.
10.4.1	**10.4.1** Critical systems have the correct and consistent time.	Shared	Comcast is responsible for using time-synchronization technology to synchornize clocks on the uCPE and backend system components. Customer is responsible for using time-synchronization technology to synchornize clocks on components in its CDE and on components connected to the uCPE.
10.4.2	**10.4.2** Time data is protected.	Shared	Comcast is responsible for using time-synchronization technology to synchornize clocks on the uCPE and backend system components. Customer is responsible for using time-synchronization technology to synchornize clocks on components in its CDE and on components connected to the uCPE.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
10.4.3	**10.4.3** Time settings are received from industry-accepted time sources.	Shared	Comcast is responsible for using time-synchronization technology to synchornize clocks on the uCPE and backend system components. Customer is responsible for using time-synchronization technology to synchornize clocks on components in its CDE and on components connected to the uCPE.
10.5	**10.5** Secure audit trails so they cannot be altered.	Shared	Comcast is responsible for securing audit trails for the uCPE and backend system components. Customer is responsible for securing audit trails for components in its CDE and for components connected to the uCPE.
10.5.1	**10.5.1** Limit viewing of audit trails to those with a job-related need.	Shared	Comcast is responsible for securing audit trails for the uCPE and backend system components. Customer is responsible for securing audit trails for components in its CDE and for components connected to the uCPE.
10.5.2	**10.5.2** Protect audit trail files from unauthorized modifications.	Shared	Comcast is responsible for securing audit trails for the uCPE and backend system components. Customer is responsible for securing audit trails for components in its CDE and for components connected to the uCPE.
10.5.3	**10.5.3** Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	Shared	Comcast is responsible for securing audit trails for the uCPE and backend system components. Customer is responsible for securing audit trails for components in its CDE and for components connected to the uCPE.
10.5.4	**10.5.4** Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	Shared	Comcast is responsible for securing audit trails for the uCPE and backend system components. Customer is responsible for securing audit trails for components in its CDE and for components connected to the uCPE.
10.5.5	**10.5.5** Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	Shared	Comcast is responsible for securing audit trails for the uCPE and backend system components. Customer is responsible for securing audit trails for components in its CDE and for components connected to the uCPE.
10.6	**10.6** Review logs and security events for all system components to identify anomalies or suspicious activity. ***Note:*** *Log harvesting, parsing, and alerting tools may be used to meet this Requirement.*	Shared	Comcast is responsible for reviewing logs and security events for the uCPE and backend system components. Customer is responsible for reviewing logs and security events for components in its CDE and for components connected to the uCPE.
10.6.1	**10.6.1** Review the following at least daily: · All security events · Logs of all system components that store, process, or transmit CHD and/or SAD · Logs of all critical system components · Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	Shared	Comcast is responsible for reviewing logs and security events for the uCPE and backend system components. Customer is responsible for reviewing logs and security events for components in its CDE and for components connected to the uCPE.
10.6.2	**10.6.2** Review logs of all other system components periodically based on the	Shared	Comcast is responsible for reviewing logs and security events for the uCPE and backend system components.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
	organization's policies and risk management strategy, as determined by the organization's annual risk assessment.		Customer is responsible for reviewing logs and security events for components in its CDE and for components connected to the uCPE.
10.6.3	**10.6.3** Follow up exceptions and anomalies identified during the review process.	Shared	Comcast is responsible for reviewing logs and security events for the uCPE and backend system components. Customer is responsible for reviewing logs and security events for components in its CDE and for components connected to the uCPE.
10.7	**10.7** Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	Shared	Comcast is responsible for retaining audit trails of the uCPE and backend system components. Customer is responsible for retaining audit trails of components in its CDE and of components connected to the uCPE.
10.8	**10.8 Additional requirement for service providers only:** Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: · Firewalls · IDS/IPS · FIM · Anti-virus · Physical access controls · Logical access controls · Audit logging mechanisms · Segmentation controls (if used)	Comcast	
10.8.1	**10.8.1** Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: · Restoring security functions · Identifying and documenting the duration (date and time start to end) of the security failure · Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause · Identifying and addressing any security issues that arose during the failure · Performing a risk assessment to determine whether further actions are required as a result of the security failure · Implementing controls to prevent cause of failure from reoccurring · Resuming monitoring of security controls	Comcast	

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
10.9	**10.9** Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.	Shared	Comcast is reponsible for security policies and operational procedures for monitoring the uCPE and backend system components. Customer is responsible for security policies and operational procedures for monitoring components in it CDE, components connected to the uCPE, and cardholder data.
11	***Requirement 11: Regularly test security systems and processes.***		
11.1	**11.1** Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. ***Note:*** *Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.* *Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.*	Shared	Comcast is reponsible for implementing processes to test for the presence of wireless access points at Comcast owned locations. Customer is responsible for implementing processes to test for the presence of wireless access points at its locations.
11.1.1	**11.1.1** Maintain an inventory of authorized wireless access points including a documented business justification.	Customer	Though implementing processes to test for the presence of wireless access points is a shared responsibility, Comcast does not use wireless access points to supprt the product, so this requirement is the sole responsibility of the customer.
11.1.2	**11.1.2** Implement incident response procedures in the event unauthorized wireless access points are detected.	Shared	Comcast is reponsible for implementing processes to test for the presence of wireless access points at Comcast owned locations. Customer is responsible for implementing processes to test for the presence of wireless access points at its locations.
11.2	**11.2** Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). ***Note:*** *Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.* *For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies:* *1) the most recent scan result was a passing scan,* *2) the entity has documented policies and procedures requiring quarterly scanning, and* *3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s).* *For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.*	Shared	Comcast is responsible for running internal and external network vulnerability scans targetting backend system components. Customer is responsible for running internal and external network vulnerability scans targetting components in its CDE and targetting the uCPE and connecting components.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
11.2.1	**11.2.1** Perform quarterly internal vulnerability scans and rescans as needed, until all "high-risk" vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel.	Shared	Comcast is responsible for running internal and external network vulnerability scans targetting backend system components. Customer is responsible for running internal and external network vulnerability scans targetting components in its CDE and targetting the uCPE and connecting components.
11.2.2	**11.2.2** Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved. ***Note:*** *Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.*	Shared	Comcast is responsible for running internal and external network vulnerability scans targetting backend system components. Customer is responsible for running internal and external network vulnerability scans targetting components in its CDE and targetting the uCPE and connecting components.
11.2.3	**11.2.3** Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.	Shared	Comcast is responsible for running internal and external network vulnerability scans targetting backend system components. Customer is responsible for running internal and external network vulnerability scans targetting components in its CDE and targetting the uCPE and connecting components.
11.3	**11.3** Implement a methodology for penetration testing that includes the following: · Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) · Includes coverage for the entire CDE perimeter and critical systems · Includes testing from both inside and outside the network · Includes testing to validate any segmentation and scope-reduction controls · Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 · Defines network-layer penetration tests to include components that support network functions as well as operating systems · Includes review and consideration of threats and vulnerabilities experienced in the last 12 months · Specifies retention of penetration testing results and remediation activities results.	Shared	Comcast is responsible for implementing a methodology for and conducting penetration tests targetting backend system components. Customer is responsible for implementing a methodology for and conducting penetration tests targetting components in its CDE and targetting the uCPE and connecting components.
11.3.1	**11.3.1** Perform *external* penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	Shared	Comcast is responsible for implementing a methodology for and conducting penetration tests targetting backend system components. Customer is responsible for implementing a methodology for and conducting penetration tests targetting components in its CDE and targetting the uCPE and connecting components.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
11.3.2	**11.3.2** Perform *internal* penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	Shared	Comcast is responsible for implementing a methodology for and conducting penetration tests targetting backend system components. Customer is responsible for implementing a methodology for and conducting penetration tests targetting components in its CDE and targetting the uCPE and connecting components.
11.3.3	**11.3.3** Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.	Shared	Comcast is responsible for implementing a methodology for and conducting penetration tests targetting backend system components. Customer is responsible for implementing a methodology for and conducting penetration tests targetting components in its CDE and targetting the uCPE and connecting components.
11.3.4	**11.3.4** If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	Shared	Comcast is responsible for implementing a methodology for and conducting penetration tests targetting backend system components. Customer is responsible for implementing a methodology for and conducting penetration tests targetting components in its CDE and targetting the uCPE and connecting components.
	11.3.4.1 Additional requirement for service providers only: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.	Comcast	
11.4	**11.4** Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	Customer	Customer is responsible for using intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into components in its CDE and into components that connect to the the uCPE.
11.5	**11.5** Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. ***Note:*** *For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre- configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).*	Shared	Comcast is responsible for deploying a change-detection mechanism for the uCPE and backend system components. Customer is responsible for deploying a change-detection mechanism for components in its CDE and for components that connecto to the uCPE.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
11.5.1	**11.5.1** Implement a process to respond to any alerts generated by the change-detection solution.	Shared	Comcast is responsible for deploying a change-detection mechanism for the uCPE and backend system components. Customer is responsible for deploying a change-detection mechanism for components in its CDE and for components that connecto to the uCPE.
11.6	**11.6** Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.	Shared	Comcast is reponsible for security policies and operational procedures for security monitoring and testing the uCPE and backend system components. Customer is responsible for security policies and operational procedures for security monitoring and testing components in its CDE and components connected to the uCPE.
12	***Requirement 12: Maintain a policy that addresses information security for all personnel.***		
12.1	**12.1** Establish, publish, maintain, and disseminate a security policy.	Shared	Comcast is responsible for establishing, publishing, maintaining, and disseminating a security policy that regards all the requirements for which it is responsible per this matrix. Customer is responsible for establishing, publishing, maintaining, and disseminating a security policy that regards all the requirements for which it is responsible per this matrix.
12.1.1	**12.1.1** Review the security policy at least annually and update the policy when the environment changes.	Shared	Comcast is responsible for establishing, publishing, maintaining, and disseminating a security policy that regards all the requirements for which it is responsible per this matrix. Customer is responsible for establishing, publishing, maintaining, and disseminating a security policy that regards all the requirements for which it is responsible per this matrix.
12.2	**12.2** Implement a risk-assessment process that: · Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), · Identifies critical assets, threats, and vulnerabilities, and · Results in a formal risk assessment. *Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.*	Shared	Comcast is responsible for implementing a risk-assessment process that is performed at least annually and upon significant changes to the uCPE and backend system component environment which identifies critical assets, threats, and vulnerabilies.. Customer is responsible for implementing a risk-assessment process that is performed at least annually and upon significant changes to components in its PCI in-scope environment which identifies critical assets, threats, and vulnerabilies relevant to those components.
12.3	**12.3** Develop usage policies for critical technologies and define proper use of these technologies. ***Note:*** *Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.* Ensure these usage policies require the following:	Shared	Comcast is responsible for developing usage policies for its critical technologies. Customer is responsible for developing usage policies for its critical technologies.
12.3.1	**12.3.1** Explicit approval by authorized parties	Shared	Comcast is responsible for developing usage policies for its critical technologies. Customer is responsible for developing usage policies for its critical technologies.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
12.3.2	**12.3.2** Authentication for use of the technology	Shared	Comcast is responsible for developing usage policies for its critical technologies. Customer is responsible for developing usage policies for its critical technologies.
12.3.3	**12.3.3** A list of all such devices and personnel with access	Shared	Comcast is responsible for developing usage policies for its critical technologies. Customer is responsible for developing usage policies for its critical technologies.
12.3.4	**12.3.4** A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)	Shared	Comcast is responsible for developing usage policies for its critical technologies. Customer is responsible for developing usage policies for its critical technologies.
12.3.5	**12.3.5** Acceptable uses of the technology	Shared	Comcast is responsible for developing usage policies for its critical technologies. Customer is responsible for developing usage policies for its critical technologies.
12.3.6	**12.3.6** Acceptable network locations for the technologies	Shared	Comcast is responsible for developing usage policies for its critical technologies. Customer is responsible for developing usage policies for its critical technologies.
12.3.7	**12.3.7** List of company-approved products	Shared	Comcast is responsible for developing usage policies for its critical technologies. Customer is responsible for developing usage policies for its critical technologies.
12.3.8	**12.3.8** Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	Shared	Comcast is responsible for developing usage policies for its critical technologies. Customer is responsible for developing usage policies for its critical technologies.
12.3.9	**12.3.9** Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use	Shared	Comcast is responsible for developing usage policies for its critical technologies. Customer is responsible for developing usage policies for its critical technologies.
12.3.10	**12.3.10** For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.	Customer	Though developing usage policies is a shared responsibility, Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
12.4	**12.4** Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	Shared	Comcast is responsible for defining information security responsibilities for all personnel in its security policies and procedures. Customer is responsible for defining information security responsibilities for all personnel in its security policies and procedures.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
	12.4.1 Additional requirement for service providers only: Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: · Overall accountability for maintaining PCI DSS compliance · Defining a charter for a PCI DSS compliance program and communication to executive management	Comcast	
12.5	**12.5** Assign to an individual or team the following information security management responsibilities:	Shared	Comcast is responsible for assigning an individual or a team for managing information security responsibilities that regard all the requirements for which it is responsible per this matrix. Customer is responsible for assigning an individual or a team for managing information security responsibilities that regard all the requirements for which it is responsible per this matrix.
12.5.1	**12.5.1** Establish, document, and distribute security policies and procedures.	Shared	Comcast is responsible for assigning an individual or a team for managing information security responsibilities that regard all the requirements for which it is responsible per this matrix. Customer is responsible for assigning an individual or a team for managing information security responsibilities that regard all the requirements for which it is responsible per this matrix.
12.5.2	**12.5.2** Monitor and analyze security alerts and information, and distribute to appropriate personnel.	Shared	Comcast is responsible for assigning an individual or a team for managing information security responsibilities that regard all the requirements for which it is responsible per this matrix. Customer is responsible for assigning an individual or a team for managing information security responsibilities that regard all the requirements for which it is responsible per this matrix.
12.5.3	**12.5.3** Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	Shared	Comcast is responsible for assigning an individual or a team for managing information security responsibilities that regard all the requirements for which it is responsible per this matrix. Customer is responsible for assigning an individual or a team for managing information security responsibilities that regard all the requirements for which it is responsible per this matrix.
12.5.4	**12.5.4** Administer user accounts, including additions, deletions, and modifications.	Shared	Comcast is responsible for assigning an individual or a team for managing information security responsibilities that regard all the requirements for which it is responsible per this matrix. Customer is responsible for assigning an individual or a team for managing information security responsibilities that regard all the requirements for which it is responsible per this matrix.
12.5.5	**12.5.5** Monitor and control all access to data.	Customer	Though assigning an individual or a team for managing information security responsibilities is a shared responsibility, Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
12.6	**12.6** Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.	Shared	Comcast is responsible for implementing a formal security awareness program to inform its personnel. Customer is responsible for implementing a formal security awareness program to inform its personnel.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
12.6.1	**12.6.1** Educate personnel upon hire and at least annually. ***Note:*** *Methods can vary depending on the role of the personnel and their level of access to the cardholder data.*	Shared	Comcast is responsible for implementing a formal security awareness program to inform its personnel. Customer is responsible for implementing a formal security awareness program to inform its personnel.
12.6.2	**12.6.2** Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	Shared	Comcast is responsible for implementing a formal security awareness program to inform its personnel. Customer is responsible for implementing a formal security awareness program to inform its personnel.
12.7	**12.7** Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.) ***Note:*** *For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.*	Shared	Comcast is responsible for screening its potential personnel prior to hire. Customer is responsible for screening its potential personnel prior to hire.
12.8	**12.8** Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:	Shared	Comcast is responsible for maintaining and implementing policies and procedures to manage its services providers. Customer is responsible for maintaining and implementing policies and procedures to manage its services providers.
12.8.1	**12.8.1** Maintain a list of service providers including a description of the service provided.	Shared	Comcast is responsible for maintaining and implementing policies and procedures to manage its services providers. Customer is responsible for maintaining and implementing policies and procedures to manage its services providers.
12.8.2	**12.8.2** Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. ***Note:*** *The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.*	Shared	Comcast is responsible for maintaining and implementing policies and procedures to manage its services providers. Customer is responsible for maintaining and implementing policies and procedures to manage its services providers.
12.8.3	**12.8.3** Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	Shared	Comcast is responsible for maintaining and implementing policies and procedures to manage its services providers. Customer is responsible for maintaining and implementing policies and procedures to manage its services providers.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
12.8.4	**12.8.4** Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	Shared	Comcast is responsible for maintaining and implementing policies and procedures to manage its services providers. Customer is responsible for maintaining and implementing policies and procedures to manage its services providers.
12.8.5	**12.8.5** Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	Shared	Comcast is responsible for maintaining and implementing policies and procedures to manage its services providers. Customer is responsible for maintaining and implementing policies and procedures to manage its services providers.
12.9	**12.9 Additional requirement for service providers only:** Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.	Comcast	
12.10	**12.10** Implement an incident response plan. Be prepared to respond immediately to a system breach.	Shared	Comcast is responsible for implementing an incident response plan for preparation for responding to a breach to the uCPE and backend system components. Customer is responsible for implementing an incident response plan for preparation for responding to a breach to components in its CDE and to components that connect to the uCPE.
12.10.1	**12.10.1** Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: · Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum · Specific incident response procedures · Business recovery and continuity procedures · Data backup processes · Analysis of legal requirements for reporting compromises · Coverage and responses of all critical system components · Reference or inclusion of incident response procedures from the payment brands.	Shared	Comcast is responsible for implementing an incident response plan for preparation for responding to a breach to the uCPE and backend system components. Customer is responsible for implementing an incident response plan for preparation for responding to a breach to components in its CDE and to components that connect to the uCPE.
12.10.2	**12.10.2** Review and test the plan, including all elements listed in Requirement 12.10.1, at least annually..	Shared	Comcast is responsible for implementing an incident response plan for preparation for responding to a breach to the uCPE and backend system components. Customer is responsible for implementing an incident response plan for preparation for responding to a breach to components in its CDE and to components that connect to the uCPE.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
12.10.3	**12.10.3** Designate specific personnel to be available on a 24/7 basis to respond to alerts.	Shared	Comcast is responsible for implementing an incident response plan for preparation for responding to a breach to the uCPE and backend system components. Customer is responsible for implementing an incident response plan for preparation for responding to a breach to components in its CDE and to components that connect to the uCPE.
12.10.4	**12.10.4** Provide appropriate training to staff with security breach response responsibilities.	Shared	Customer is responsible for implementing an incident response plan for preparation for responding to a breach to components in its CDE and to components that connect to the uCPE.
12.10.5	**12.10.5** Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion- prevention, firewalls, and file-integrity monitoring systems.	Shared	Comcast is responsible for implementing an incident response plan for preparation for responding to a breach to the uCPE and backend system components. Customer is responsible for implementing an incident response plan for preparation for responding to a breach to components in its CDE and to components that connect to the uCPE.
12.10.6	**12.10.6** Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	Shared	Comcast is responsible for implementing an incident response plan for preparation for responding to a breach to the uCPE and backend system components. Customer is responsible for implementing an incident response plan for preparation for responding to a breach to components in its CDE and to components that connect to the uCPE.
12.11	**12.11 Additional requirement for service providers only:** Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: · Daily log reviews · Firewall rule-set reviews · Applying configuration standards to new systems · Responding to security alerts · Change management processes	Comcast	
12.11.1	**12.11.1 Additional requirement for service providers only:** Maintain documentation of quarterly review process to include: · Documenting results of the reviews · Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program	Comcast	