LUMEN DISTRIBUTED DENIAL OF SERVICE MITIGATION SERVICE
SERVICE SCHEDULE

1. General. This Service Schedule is applicable only where Customer orders Distributed Denial of Service Mitigation Service ("DDoS Mitigation Service"), Lumen® DDoS Hyper® or Application Protection Services (collectively, "Services") provided by Lumen. "Lumen" is defined for purposes of this Service Schedule as CenturyLink Communications, LLC d/b/a Lumen Technologies Group or its affiliated entities. Distributed Denial of Service Mitigation Service may be designated as "DDoS," "Denial of Service," "Distributed DoS Service," "DDoS Mitigation Service" or "Distributed DoS Mitigation Service" in Orders, Order acceptance, service delivery, billing and related documents. Application Protection Services may also be referred to as Web Application and API Protections, WAF services and/or Web Application Firewall services in Orders, Order acceptance, service delivery, billing and related documents. Certain DDoS Mitigation Service features orderable online via self-serve may be referred to as "Lumen® DDoS Hyper®" or "DDoS Hyper". In addition, certain Application Protection Services are orderable online via self-serve, so long as Customer is also purchasing DDoS Hyper. This Service Schedule incorporates the terms of the Master Service Agreement or other service agreement under which Lumen provides the Services to Customer (the "Agreement"). If a conflict exists among the provisions of the Service Attachments, the order of priority will be this Service Schedule, the Agreement, the Service Guide, and the Order(s). Certain Services are subject to geographic and/or feature availability and may require additional terms and may be provided by Lumen's vendor.

1.1 Additional General Terms. Service charges are exclusive of taxes and presented without reduction for any Withholding Tax, all of which are the responsibility of the Customer. "Withholding Tax" means any amount or account of tax on sources of income which a payor is obliged to deduct from payments due to a recipient and account for or to any tax authority. In the event that any payment to be made to Lumen under this Service Schedule should be subject to reduction by reason of a Withholding Tax, Customer agrees to pay Lumen such amounts as would have been necessary so that the aggregate net amount received by Lumen after application of a Withholding Tax is the same amount as would have been received by Lumen if there had been no requirement to deduct or withhold such tax. For Services provided outside the United States, Customer or its local affiliate may be required to enter into a separate local country addendum/agreement (as approved by local authorities) ("LCA") with the respective Lumen affiliate that provides the local Service(s). Such Lumen affiliate will invoice Customer or its local affiliate for the respective local Service(s).

2. Services.

2.1 DDoS Mitigation Service.

2.1.1 DDoS Mitigation Service is available on Customer's separately purchased Internet services. The Order will specify the type of DDoS Mitigation Services and whether the Services are Always-On or On-Demand. Additional DDoS Mitigation Service options that Customer will select and that will be identified in the Order are listed below or in the Service Guide.

2.1.2 DDoS Mitigation Service includes and protects Customer IP addresses up to a combination of 256 /24 of IPv4 or 256 /48 of IPv6. Unlimited protected IP addresses, which may also be referred to as unlimited address space size or unlimited address space, are optional and can be purchased for an additional monthly recurring charge.

2.1.3 Additional features or functionality described in an Order, and not described or referenced in this Service Schedule will be provisioned at then current rates pursuant to Lumen's then-current Service Schedule and/or Service Guide applicable to the features or functionality, both of which are located at https://www.lumen.com/en-us/about/legal/business-customer-terms-conditions.html.

2.1.4 Notwithstanding anything in the Agreement to the contrary, Lumen may, in its sole and absolute discretion, use a vendor for any or all of the work to be performed (e.g. installation) or Services provided (e.g. Application Protection Services) under this Service Schedule, provided that Lumen will remain responsible for the performance of its obligations in this Service Schedule. Services that work in conjunction with DDoS Mitigation Services (i.e. internet services) are subject to separate Service Schedules.

2.1.5 On-Demand Service. For On-Demand Service, once the Mitigation Infrastructure is engaged, if an identifiable Attack is not seen by Lumen within 48 hours, Lumen will coordinate with Customer and obtain consent from Customer (which will not be unreasonably withheld) to return Customer to normal conditions. Upon receipt of Customer consent, Lumen may continue to maintain traffic on Mitigation Infrastructure for an agreed-upon limited time period. Upon confirmation of an Attack and with the cooperation of Customer, Lumen will route Customer's IP traffic to the Mitigation Infrastructure designed to filter malicious Attack traffic and pass through legitimate traffic in order to Mitigate the potential disruptions caused by an Attack. However, due to the varying nature of Attacks, Lumen cannot warrant that all Attacks will be detected and/or Mitigated; nor does Lumen warrant that all IP traffic patterns that initially appear to be Attacks are actual Attacks.

2.1.6 Always-On Service. For Always-On Service, the diverted traffic entering Lumen's Mitigation Infrastructure will be inspected and filtered of Attack traffic based on predefined filters agreed upon by Lumen and Customer. Customer must report to Lumen any new Attacks not effectively blocked by predefined filters. Lumen will respond to new requests for Mitigation in accordance with the TTM SLA.

2.1.7 DDoS Hyper. DDoS Hyper is a version of DDoS Mitigation Service only available through Lumen's digital buying experience. DDoS Hyper is available in two tiers, DDoS Hyper Essentials and DDoS Hyper Plus as defined in the Service Guide.

2.2 Application Protection Services. Application Protection Services collectively refers to a set of software applications (i.e. all provided as software as a service) made available through Lumen and more fully described in the Service Guide. Application Protection Services utilizes DNS entry updates as a mechanism to enable access to Application Protection Service. Lumen will assign virtual IP addresses ("VIPs") that the Customer will point to either directly or via another DNS record. Customer is responsible for updating Customer's DNS entries to Lumen-provided information in order to access the Service. Application Protection Service requires Customer to provide Lumen with a SSL certificate for each software application purchased by Customer.

2.3 Service Level Agreements ("Service Levels").

The following Service Levels are not available until completion of Service Validation. Whether a Service issue constitutes an outage or failure for Service credit purposes will be determined by Lumen on the basis of available records, data and other evidence, including through the use of third party monitoring tools. Credits are only available against the MRC for the affected Service. The Service Levels stated below apply to the Mitigation aspect of Service. Service Levels do not apply to any Service features not expressly identified in this section, or Service outages or failures due to Excused Outages, Suspension or Chronic Problems.

(A) DDoS Mitigation Service Levels, Service Credits and Chronic Outages. Lumen will use commercially reasonable efforts to ensure the Mitigation Infrastructure is available to Customer one hundred percent (100%) of the time once Customer's IP traffic is routed to the Mitigation Infrastructure in response to a confirmed Attack and until Customer's IP traffic is re-routed back to normal following cessation of the Attack (the "Mitigation SLA"). For purposes of this Mitigation SLA, a "Mitigation Service Outage" means that the Mitigation Infrastructure is unavailable to Customer to the extent that Customer is routing traffic through the Mitigation Infrastructure (*i.e.,* the Customer cannot pass traffic through the Mitigation Infrastructure) for more than 60 consecutive seconds. If the Mitgation SLA is not met, the following remedies will apply:

Mitigation Service Outage Duration	Service Credit
>60 consecutive seconds ≤4 consecutive hours	3 days of the MRC*
>4 consecutive hours	5 days of the MRC*

*The Service credit is based on the MRC associated with the affected Service at the affected location. Per day calculation based on a 30 day calendar month.

In no event will Customer receive a credit for more than one (1) Mitigation Service Outage per day pursuant to the terms of this Section 2.3 (A), regardless of the number of times Lumen fails to comply with the Mitigation SLA during that day.

Chronic Outages. In addition to the above credit(s), Customer will be entitled to terminate the affected DDoS Mitigation Service without early termination liability within 30 calendar days of the date/time the right of termination is triggered if any of the following apply:

(i) a single, continuous Mitigation Service Outage extends for 10 or more consecutive days; or

(ii) 7 separate Mitigation Service Outages each lasting at least 60 minutes in a 90 day period; and

(iii) if Customer has separately procured from Lumen an IPVPN circuit or Lumen Internet Service circuit as part of the DDoS Mitigation Service, Customer's termination rights in this Service Schedule extend to the applicable IPVPN Service or Lumen Internet Service.

(B) DDoS Mitigation Service Time to Mitigate ("TTM") Service Level ("SLA"). Lumen agrees to deploy Mitigation following Customer approval (which may be verbal) and Customer properly routing traffic to the Mitigation Infrastructure during an Attack. The TTM SLA is measured in minutes commencing from either (i) the time Lumen obtains Customer approval and Customer properly routing traffic to the Mitigation Infrastructure during an Attack, or (ii) the time of automated initiation by Flow Based Monitoring ("FBM") to route Customer's traffic to the Mitigation Infrastructure when an Attack is detected ("Auto-Mitigation") until the time (in minutes) Lumen deploys countermeasures to initiate Mitigation. The applicable TTM SLA for each type of Attack is set forth below.

Attack Type	TTM SLA for On-Demand without Auto-Mitigation	TTM SLA for On-Demand with Auto-Mitigation	TTM SLA for Always-On
UDP/ICMP Floods SYN Floods TCP Flag Abuses DNS Reflection DNS Attack HTTP GET/POST Attacks*	10 minutes	5 minutes	2 minutes

*HTTP Get/Post Attack Mitigation requires a subscription to the Web Application Firewall and BOT Management (WAF/BOT) service .

If the TTM SLA is not met, the following remedies apply:

Time to Initiate Mitigation	Service Credit
>10 minutes ≤ 60 minutes	1 day of the MRC*
>60 minutes ≤ 6 hours	2 days of the MRC*
>6 hours	7 days of the MRC*

*The Service credit is based on the MRC associated with the affected Service at the affected location. Per day calculation based on a 30 day calendar month.

If the TTM SLA is not achieved three or more times in a single day, Lumen will provide a single credit for that day equal to the maximum 7 days of the MRC credit.

If 3 or more TTM SLAs are not met during a calendar month, in addition to Service credits, Customer will have the right to terminate the applicable Service without early termination liability; provided that the right of termination is exercised wtihin 30 days following the date/time the right of termination is triggered.

Customer is deemed to have pre-approved Mitigation for the Auto-Mitigation option or Always-On and the SOC does not have to call Customer for permission to start Mitigation. Certain mitigation countermeasures related to FBM Service may be pre-authorized by Customer. If a countermeasure is required that has not been pre-authorized (e.g. in addition to the pre-authorized countermeasures), verbal approval is required from Customer to deploy such countermeasure.

Mitigation requiring traffic analysis and custom signature development are not covered under the TTM SLA.

(C) DDoS Mitigation Service Attack Monitoring Services Time to Notify Service Level (FBM and AMM Cloud Signaling Services only).

If Customer orders FBM Service or AMM Cloud Signaling Service, Customer may request a credit as set forth below if an Attack Monitoring Failure to Notify Event ("FTN Event") occurs. An FTN Event is an Event in which an Attack Monitoring DDoS alert occurs but steps to notify Customer within a period of 15 minutes from the time that Lumen receives a "Type DDoS" alert are not taken. Timely efforts to notify Customer whether via email or phone satisfy the requirement to take such steps whether or not the Customer can be reached.

For each FTN Event that occurs during a calendar month, upon Customer request Lumen will provide a service credit equal to the pro-rated charges for 3 days of the MRC applicable to the affected Service. If 3 or more FTN Events occur during a calendar month, in addition to service credits, Customer will have the right to terminate the affected FBM Service or AMM Cloud Signaling Service without early termination liability; provided that the right of termination is exercised wtihin 30 days following the date/time the right of termination is triggered.

(D) General Terms for all Service Levels.

Lumen continually makes improvements to the Service and reserves the right to make any updates, error corrections, bug fixes, and other modifications to any software, equipment or hardware utilized by Lumen to provide the Services, at any time. Lumen will use reasonable efforts to make such changes during the Regularly Scheduled Maintenance window.

To be eligible for SLA credits, Customer must be current in its obligations, and Customer must contact Lumen Billing Inquiries via the contact information provided on their invoice, open a ticket in the Portal or contact their account manager to report any issue for which Customer thinks a Service Level may apply within 30 calendar days after the issue occurs. Credits will not apply to any custom service. Duplicative credits (e.g., for both a Mitigation SLA and a TTM SLA) will not be awarded for a single failure or outage. If a single failure or outage triggers both the Mitigation SLA and TTM SLA, Customer will be entitled to receive the higher of the two credits. The aggregate credits under subparts (A), (B) and (C) above to be provided in any calendar month will not exceed 100% of the MRC of the affected Service. Cumulative credits in any one month must exceed $100.00, or local currency equivalent, to be processed. The Service credits and termination rights stated in this Service Schedule will be Customer's sole and exclusive remedies with respect to the DDoS Mitigation Service and related Services provided under this Service Schedule.

3. Customer Responsibilities. Lumen will not be liable for any failure to perform due to Customer's failure to fulfill Customer's responsibilities and requirements as detailed in this Service Schedule or due to Customer's errors or omissions in setting up the environment.

3.1 Charges.

3.1.1 Unless otherwise provided in the Service Guide, Service will be billed monthly in advance. DDoS Mitigation Service rates are up to a predefined bandwidth level designated on the Order. Charges consist of 2 components: (a) a non-recurring charge, ("NRC", "One Time Charges", or similar references"), if applicable, and (b) a monthly recurring charge ("MRC", "Monthly Charge", or similar references).

3.1.2 Lumen reserves the right to use dynamic exchange rates to calculate all non-USD billing. This means that the exchange rate published on the day each respective monthly invoice is created will be the exchange rate used to appropriately convert the invoiced amounts from USD to the applicable currency. In the alternative, Lumen reserves the right to adjust the exchange rates on a regular basis (e.g., monthly). Exchange rate adjustments will not be deemed a rate adjustment.

3.1.3 Expedite Service. Certain DDoS Mitigation Services are eligible for expedited "turn-up" of Service for an additional one-time charge ("Expedited Service"). Customer acknowleges and agrees that requesting the Expedited Services means acceptance of the DDoS Mitigation Services for the Service Term specified in the Order and cooperating with Lumen to ensure the DDoS Mitigation Services ordered can be installed and provided. If Customer does not cooperate and accept the Services after the Expedited Services have been turned up, Customer will be billed and agrees to pay 100% of the MRC multiplied by the number of months remaining in the Service Term. Lumen will exercise good faith efforts to turn up Expedited Service for GRE Service in one (1) business day; however this is a nonbinding objective. For DDoS Mitigation Service other than GRE Service, the Order will be processed in a prioritized manner. If Customer orders

Expedited Service, there is no Portal access and no Service Levels will apply to Expedited Service during the first seven (7) days of service.

3.1.4 Lumen reserves the right to suspend Expedited Service, DDoS Mitigation Services and/or DDoS Hyper at any time if Customer fails to satisfy credit requirements which may be imposed after the completion of a credit review; even if Service is provisioned.

3.2 Service Commencement Date.

3.2.1 The Service Commencement Date for DDoS Mitigation Service begins on the date stated on the Connection Notice. The Connection Notice for DDoS Mitigation Service will be issued either upon: (i) successful completion of Service Validation or (ii) after Lumen has provisioned all components of the Service that Lumen can provision without Customer's assistance. If there are multiple locations, billing for each location will automatically begin when Lumen completes provisioning. No additional Connection Notices will be provided. Charges for certain Services are subject to (a) a property tax surcharge and (b) a cost recovery fee per month to reimburse Lumen for various governmental taxes and surcharges. Such charges are subject to change by Lumen and will be applied regardless of whether Customer has delivered a valid tax exemption certificate. For additional details on taxes and surcharges that are assessed, visit www.lumen.com/taxes.

3.2.2 The Service Commencement Date for Application Protection Service is the date stated on the Connection Notice, which is 21 calendar days after issuance of a Connection Notice. The Connection Notice will be issued when the applicable software is made available for Customer's use.

3.2.3 The Service Commencement Date for DDoS Hyper begins on the date stated on the Connection Notice, which is 5 calendar days after issuance of a Connection Notice. The Connection Notice is issued when at least 1 clean traffic return path has been provisioned.

3.3 Term; Renewal; Termination. This Section 3.3 applies in lieu of any other term, cancellation, and termination section, including any available rights of termination that may be in the Agreement.

3.3.1 Term; Renewal. DDoS Mitigation Service and Application Protection Services have a minimum term which begins on the Service Commencement Date and continues for the period set forth in the Order ("Service Term"). SOC Advanced Support Services have a month-to-month term. Except for Application Protection Services, which automatically expire at the end of the Service Term, DDoS Service will automatically renew for subsequent month to month terms upon expiration of the initial Service Term. Renewal terms for third party software may be determined by the applicable third-party provider.

3.3.2 Termination. If DDoS Mitigation Service is terminated either by Lumen as a result of Customer's default or by Customer for any reason other than Lumen's default, and prior to the conclusion of the applicable Service Term, then Customer will be liable for the early termination charges set forth in the Agreement. If Application Protection Service is terminated prior to expiration of the applicable Service Term, either as part of a DDoS Mitigation Service termination or independently, Customer is responsible for 100% of the MRCs multiplied by the number of months remaining in the Service Term. Customer is fully responsible for updating DNS entries to no longer point to Application Protection Services prior to any termination date, whether it is requested by Customer or Lumen, and failure to do so will make the website inaccessible.

3.3.3 Subject to the early termination charges section above, if DDoS Mitigation Service is terminated for any reason, all other related Services provided under this Service Schedule will also be terminated; provided however Application Protection Services may continue to be provided to Customer independently of DDoS Mitigation Service. Customer may independently terminate Application Protection Services without affecting any in term DDoS Mitigation Services.

3.4 IP Addresses. If Lumen or an applicable Lumen vendor, grants to Customer a right to use an IP address as part of the provision of Service, Customer acknowledges and agrees the IP address is owned or leased by Lumen or the applicable Lumen vendor and the IP address will revert to Lumen or the applicable Lumen vendor after termination of the applicable Order for any reason whatsoever, and Customer will cease using the IP address. At any time after termination, Lumen or the applicable Lumen vendor may re-assign IP address(es) to another user.

If Lumen does not assign to Customer an IP address as part of the provision of Service, Customer represents and warrants that all title, right and interest in and to each IP address used by Customer in connection with the Service is owned exclusively by Customer and/or Customer has all permissions necessary from the owner to enable Lumen and Customer to perform their obligations. Customer wll defend Lumen and its affiliates from any claim, demand or action arising in connection with a breach of the foregoing warranty. Customer will also pay any costs of settlement, or any damages finally awarded by a court of competent jurisdiction against Lumen and payable to such third party as a result of such claim.

3.5 Customer Information. Customer must provide and maintain an English-speaking point of contact with current, complete, and accurate contact information at all times that is reachable 24/7 for the Service's required notifications, including for set-up and installation and should be authorized to consent to make or direct changes to the Customer's security infrastructure or architecture, as applicable.

3.6 Customer must cooperate with Lumen and Lumen's vendors in coordinating setup of the DDoS Mitigation Service, including but not limited to, placing the necessary routing device at the edge of Customer's environment and cooperating with Lumen in the rerouting of IP traffic to the Mitigation Infrastructure during an Attack.

3.7 Notification Responsibilities. Customer must provide Lumen with all the following notices: (i) 24 hours advance notice of any potential promotional events or other activities that may increase Customer's network or website traffic; (ii) immediate notice of any sudden events that may cause significant IP traffic pattern changes in Customer's network; (iii) 24 hours advance notice of any Customer requests to change the traffic baseline; (iv) immediate notice of any additions or deletions to the list of Customer IP addresses subject to the Service; (v) immediate notice if Customer believes it is under a DDoS Attack and provide Lumen with reasonable assistance to reroute the IP traffic to the Mitigation Infrastructure; (vi) immediate notice related to any changes to Customer's contact information, including email; and (vii) at least five (5) business days of any network topology or system changes that may affect the Service utilization or the effectiveness of the DDoS Mitigation counter-measures to avoid potential Service impacts. For changes that are Service or price impacting, changes must be agreed to in a new Order before the change will go into effect. If Customer doesn't comply with its notification responsibilities or if Customer performs system changes without prior notification to Lumen. Lumen may not be able to provide the Service, or the Service may not function properly, including the inability to monitor traffic or the generation of false alerts. Lumen will work with the Customer to resolve chronic false positives and other nuisance alerts; however, if alerting issues are not resolved satisfactorily, Lumen may modify the DDoS Mitigation system configuration to reduce repetitive alarms caused by Customer system changes.

3.8 Due to the varying nature of malicious activity, Lumen cannot guarantee that all malicious activities intended to be blocked will be identified, detected and blocked. Customer must establish and consistently maintain reasonable and adequate security policies and devices for defense of its assets. Customer acknowledges that the Services are regarded as a tool that can be used as part of the Customer's overall security strategy, but not as a total solution. Customer acknowledges that Customer, and not Lumen, is responsible for Customer's own network security policy and security response procedures.

3.9 Customer understands and expressly consents that in the performance of its obligations in this Service Schedule, notwithstanding any other requirements in the Agreement between Lumen and Customer, Lumen (or its vendors) may route Customer traffic to the Mitigation Infrastructure which is located in a country other than the country of origination and/or destination of such traffic.

3.10 If Customer or Lumen detect the Service is being affected by a continuing error, conflict or trouble report, or similar issue (in each case a "Chronic Problem") caused by the Customer, Customer will resolve any Chronic Problem by taking whatever steps are deemed necessary to rectify the same, including, but not limited to: (i) removing or modifying the existing Service configuration (or requesting Lumen to remove the same); or (ii) replacing Customer's equipment providing distributed denial of service Mitigation should that be deemed necessary. If Customer has not remedied the Chronic Problem within 30 days of request by Lumen, then Lumen may suspend or terminate the Service. The SLA will not apply and Customer will not be entitled to receive a credit or exercise a termination right under the SLA during periods of of Chronic Problems caused by Customer.

3.11 Installation/Setup. Customer will cooperate with Lumen by providing Lumen with all information concerning the Service reasonably requested by Lumen and a point of contact. Customer will provide data parameters that will allow Lumen to determine the proper threshold levels in an attempt to diagnose a DDoS Attack. Lumen may periodically require Customer to allow traffic monitoring to determine proper threshold levels.

3.12 Software. If any third-party software, including any corresponding documentation, is provided to Customer by Lumen in connection with the Service, Customer will defend Lumen and its affiliates from any claim, demand or action arising in connection with Customer's failure to use third party software in a manner not authorized by this Service Schedule. Customer will also pay any costs of settlement, or any damages finally awarded by a court of competent jurisdiction against Lumen and payable to such third party as a result of such claim. Customer acknowledges and agrees that it is solely responsible for selecting and ensuring that Customer provided software and systems are up to date and supportable. Customer is solely responsible for the installation, operation, maintenance, use and compatibility of the Customer provided software or systems. Customer's failure to do so may result in Lumen's inability to provide the Services and Lumen will have no liability therefrom, including for missed Service Levels.

For any third-party software designated Third Party Software or Service, Lumen offers quoting, ordering, and billing only. Customer acknowledges that fees, payment, pricing, billing, tax, and early termination terms are governed by the Agreement and this Service Schedule and Lumen reserves the right to exercise all available remedies under the Agreement, including Suspension or termination for non-payment. Customer will be required to agree (i.e., express, active acceptance or passive acceptance via these terms) to the applicable software licensor's or vendor's then current standard terms and conditions as a condition of having access to the Third-Party Software or Service.

3.13 Customer consents to Lumen and the applicable vendors or licensors collecting and compiling system and operational metrics data to determine trends and improve service capabilities. Lumen and its vendors and/or licensors may associate this data with similar data of other Customers so long as the data is merged in a manner that will not in any way reveal the data as being attributable to any specific Customer.

3.14 Testing. Customer will not attempt, permit, or instruct any party to take any action that would reduce the effectiveness of the Service. Without limiting the foregoing, Customer is specifically prohibited from conducting unannounced or unscheduled test DDoS Attacks, penetration testing, or external network scans on Lumen's network without the prior written consent of Lumen.

3.15 Change Request. Customers must request non-price impacting Service changes by opening a ticket or by contacting the SOC. Customers must provide complete authentication credentials when requesting changes. Any non-emergency changes or service design changes that may be required outside of an Attack such as prefix additions and migration from On-Demand to Always-On require a change order.

Customers ordering Lumen® DDoS Hyper® must make changes to configurations, features and bandwidth via the online self-service interface. Changes to DDoS Hyper via the Portal that reduce the initial Service Term are not valid until the initial term is fulfilled.

3.16 Neither Customer nor its representatives will attempt in any way to circumvent or otherwise interfere with any security precautions or measures of Lumen relating to the Service or any other Lumen equipment.

3.17 Customers who have published RPKI ROAs are responsible for updating the Route Registry associated with their IP space and AS number to permit Lumen to advertise the applicable IP address to help ensure proper routing of legitimate traffic. If Customer does not update the registry accordingly Lumen's ability to mitigate some or all Attack(s) on Customer's IP address will be reduced.

3.18 Portal Use. If Lumen provides Customer with Portal access in connection with the Service, Customer will use access solely for use with the Service in accordance with this Service Schedule and the Agreement, and Customer will be responsible for any unauthorized access to or use thereof unless Customer can prove that access or use has not been caused by any culpable action or omission of Customer or attributable to Customer. A monthly recurring charge will apply to any Customer users in excess of ten (10) Customer users of the Service Portal. The Service uses two-factor authentication ("2FA") for access to the Portal. Customer must install two-factor authentication software to be used for validating identity while interacting with the Portal. Access to Portal may be disabled for accounts that have not been active in more than six (6) months requiring such users to contact Lumen if they wish to reestablish access. In addition, as is part of any support requested by Customer, Lumen may need to access Customer information within the Portal and Customer's request for support constitutes its consent for Lumen to access the Portal information as needed.

4. Additional Service Limitations and Disclaimers.

4.1 Intellectual Property. If Lumen develops or creates any intellectual property as part of DDoS Mitigation Services ("DDoS Intellectual Property"), that DDoS Intellectual Property will be, and remain, the exclusive property of Lumen and will not be considered a work for hire. DDoS Intellectual Property includes, by way of example, playbooks, runbooks, reports, operational processes, and Lumen equipment configuration settings. Customer will have no right to sell, lease, license or otherwise transfer, with or without consideration, any DDoS Intellectual Property to any third party or permit any third party to reproduce or copy or otherwise use or see the DDoS Intellectual Property in any form and will use all reasonable efforts to ensure that no improper or unauthorized use of the DDoS Intellectual Property is made. Customer will not reverse engineer or de-compile any DDoS Intellectual Property, unless expressly permitted by applicable law. Customer will promptly, upon termination of this Service Schedule or upon the request of Lumen, deliver to Lumen all DDoS Intellectual Property without retaining any copy or duplicate; except that Customer may keep a copy of any report(s) provided by SOC Advanced Support, which may previously have been referred to as PSSA subject to prior approval of Lumen and treatment of the reports as "confidential" pursuant to the terms of the Agreement. Customer is expressly prohibited from using any component of the DDoS Mitigation Service or DDoS Intellectual Property other than as expressly provided for in this Service Schedule.

4.2 Privacy/Data Protection. Customer acknowledges that Lumen may process personal information of Customer and/or its end users in connection with providing, monitoring, and managing the Services, including across national borders. Lumen may also disclose such information to its affiliates and underlying vendors for similar processing in connection with providing the Service or to comply with applicable law. Customer is responsible for complying with all privacy and data protection laws and regulations regarding Customer content, end users, and other relevant data Customer elects to process via the Services, including ensuring a valid legal basis and adequate notifications for all such processing. Customer is solely responsible for properly configuring and using the Service and taking its own steps to maintain appropriate security controls, information protection, and backup (if applicable) of any data, which may include the use of encryption technology to protect such data from unauthorized access or use. Given that Customer determines which data to process via the Service and which security measures to apply to such data, notwithstanding anything else to the contrary in this Service Schedule or the Agreement, Customer and not Lumen will be responsible for whether the Services are suitable to process the relevant data.

4.3 Additional Disclaimer of Warranty; Liability.

4.3.1 Customer acknowledges the Services endeavor to Mitigate security Events, but Events, even if determined to be Attacks, may not be mitigated entirely, or rendered harmless. Customer further acknowledges that it should consider the Service as just one tool to be used as part of an overall security strategy and not a guarantee of security. The Service provided in this Service Schedule is a supplement to Customer's existing security and compliance frameworks, network security policies and security response procedures, for which Lumen is not, and will not be, responsible. While Lumen will use reasonable commercial efforts to provide the Services in accordance with the SLA, the Services are otherwise provided "as-is." LUMEN MAKES NO WARRANTY, GUARANTEE, OR REPRESENTATION, EXPRESS OR IMPLIED, THAT ALL SECURITY THREATS AND VULNERABILITIES WILL BE DETECTED, THAT THE PERFORMANCE OF THE SERVICES WILL RENDER CUSTOMER'S SYSTEMS INVULNERABLE TO SECURITY BREACHES, THAT ANY THIRD PARTY SOFTWARE PROVIDED BY CUSTOMER WILL BE COMPATIBLE WITH THE SERVICE AND/OR THAT LUMEN'S PERFORMANCE OF SECURITY SERVICES, INCLUDING ACTIVITIES OR TASKS WILL COMPLY WITH OR SATISFY ANY APPLICABLE GOVERNMENTAL OR INDUSTRY DATA SECURITY STANDARD. IF ACTIVITIES OR TASKS INCLUDE BY WAY OF EXAMPLE, MAKING RECOMMENDATIONS, PERFORMING ASSESSMENTS, TESTS, OR PROVIDING REPORTS CUSTOMER AGREES THAT SUCH ACTIVITIES ARE PROVIDED IN GOOD FAITH AS TO ITS ACCURACY A AND LUMEN DOES NOT AND CANNOT GUARANTEE THAT SUCH ACTIVITIES, RECOMMENDATIONS, ASSESSMENTS, TESTS OR MONITORING WILL BE ACCURATE, COMPLETE, ERROR-FREE, OR EFFECTIVE IN ACHIEVING CUSTOMER'S SECURITY AND/OR COMPLIANCE RELATED OBJECTIVES. ALL PROFESSIONAL SECURITY ASSISTANCE SERVICES ARE PROVIDED AS IS. Neither Lumen or its vendors will be liable for any damages or liabilities however classified including third party claims which Customer or third parties may incur as a result of: (i) non-

compliance with any standards which apply to Customer, and/or (ii) reliance upon (or implementation of recommendations from) results, reports, tests, or recommendations related to the Services; or (iii) loss or corruption of data or information transmitted through the Service.

4.3.2 THIRD PARTY SOFTWARE OR SERVICES ARE NOT PART OF THE SERVICE, AND CUSTOMER ACQUIRES THEM DIRECTLY FROM THE THIRD-PARTY PROVIDER. LUMEN IS NOT RESPONSIBLE OR LIABLE FOR ANY DAMAGES WHATSOEVER RELATED TO THIRD PARTY SOFTWARE OR SERVICES, EVEN IF LUMEN RECOMMENDS THE THIRD PARTY PROVIDER, EVEN IF THE THIRD PARTY SOFTWARE OR SERVICE IS RELATED TO THE SERVICE OR TO CUSTOMER'S ABILITY TO RECEIVE OR EXPLOIT THE SERVICE, AND EVEN IF LUMEN ACTS AS THE THIRD PARTY PROVIDER'S AGENT IN DELIVERING OR ENABLING ACCESS TO THE THIRD PARTY SOFTWARE OR SERVICE, IN COLLECTING PAYMENT, OR IN OTHER WAYS. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, LUMEN WILL HAVE NO RESPONSIBILITY OR LIABILITY FOR MAINTENANCE, UPDATES, OR UPGRADES OF THIRD-PARTY SOFTWARE AND SERVICES, FOR INTELLECTUAL PROPERTY INFRINGEMENT BY THIRD PARTY SOFTWARE OR SERVICES OR ANY FAILURE OR PERFORMANCE OF THE THIRD-PARTY SOFTWARE OR SERVICE. Lumen is the applicable supplier's agent for purposes of ordering, collecting payment or in other ways as it relates to third party software or Services.

4.3.3 Direct Damages. Except for the payment and indemnification obligations of Customer and subject to the Liability Limitations and Exclusions provision in the Agreement or similar waiver of consequential damages provision, the total aggregate liability of each party arising from or related to this Service Schedule will not exceed the total MRCs, NRCs, and usage charges paid or payable to Lumen for the affected Services under this Service Schedule in the six months immediately preceding the first event giving rise to the cause of action ("Damage Cap").

4.4 Suspension; Access; Restrictions.

4.4.1 Lumen may temporarily suspend any Service immediately if Lumen has a good faith belief that Suspension is reasonably necessary to Mitigate damage or liability to the Mitigation Infrastructure or Lumen network or to other customers of Lumen that may result from Customer's continued use of the Service. In addition to any rights or obligations of the parties due to regulatory changes in the Agreement, Lumen may terminate any Order if Lumen or an applicable vendor or subcontractor cannot maintain any required regulatory approvals, despite its reasonable efforts to do so. Customer's access to the applicable Services will end as of the effective date of termination or expiration and Services do not include transition assistance.

4.4.2 Nothing in this Service Schedule or the Agreement grants Customer any rights to, and Customer is expressly prohibited from, reselling the Services or using any component of the Service or any Lumen proprietary materials to create or offer derivative versions of the Service either directly, or through a third party, as a standalone service offering, as bundled with Customer's services or products, or on a service-bureau basis.

4.4.3 Customer understands that DDoS Mitigation Service may result in disruptions of and/or damage to Customer's, Customer's end-users' or third parties' information systems and the information and data contained therein, including but not limited to denial of access to a legitimate system user. The Services do not include backing up data prior to deploying Services or for arranging alternative means of operation should such disruptions or failures occur. Customer understands and acknowledges that the Service is not suitable for the maintenance or processing (apart from mere transmission) of protected health information consistent with the Health Insurance Portability and Accountability Act (HIPAA), as amended or any other applicable laws in the matter.

5. Definitions. Any capitalized terms used in this Service Schedule or Service Guide and not otherwise defined will have the meanings set forth in the Agreement.

"Always-On" refers to an optional feature for DDoS Mitigation Direct, DDoS Mitigation Internet Direct Service, or DDoS Mitigation GRE Service that continually diverts Customer's inbound internet traffic through the Mitigation Infrastructure using BGP networking service.

"Attack" means a distributed denial of service attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system.

"Event" means a security abnormality detected by the Service or reported by Customer to the SOC. An Event does not necessarily constitute an actual security incident or Attack and must be investigated further to determine its validity.

"Excused Outage" will also mean for purposes of this Service Schedule, and in addition to the Agreement, the SLA will not apply, and Customer will not be entitled to receive a credit or exercise a termination right under the SLA, for any outage that adversely impacts the Service that is caused by, or attributable to: (a) the acts or omissions or misuse of the Service by Customer, its employees, contractors or agents or its end users; (b) the failure or malfunction of equipment, applications, the public Internet or other network or telecommunications unavailability, or systems not owned or controlled by, or attributable to, Lumen; (c) Regularly Scheduled Maintenance or emergency maintenance, alteration or implementation; (d) the unavailability of required Customer personnel or the inability of Lumen to contact Customer related to the Service, including as a result of failure to provide Lumen with accurate, current contact information (including email); (e) Lumen's lack of access to the Customer premises where reasonably required to restore the Service; (f) Customer's failure to release the Service for testing or repair and continuing to use the Service on an impaired basis; (g) Customer's failure to provide timely approvals and/or consents, including allowing Lumen to retune the Service as required for Lumen to provide the Service; (h) Customer's sustained traffic load reaching a point that causes material degradation to or outage of the underlying Lumen Internet infrastructure not directly related to the Mitigation Infrastructure; (i) improper or inaccurate network specifications provided by Customer;

(i) Customer is in breach of its obligations under the Agreement or this Service Schedule; (j) Customer failure to properly update the Route Origin Authorization ("ROA"); or (k) Customer's failure to notify Lumen in advance of network topography or system issues if the failure to notify results in failures, interruptions or degradation of Service.

"Mitigation" or "Mitigate" means rerouting of traffic through Lumen DDoS Mitigation Service and initiating countermeasures with the intent to remove Attack traffic identified by the Mitigation Infrastructure located in Lumen's network.

"Mitigation Infrastructure" is defined as a collection of Lumen devices consisting of routers, servers and scrubbers that connect to Lumen's internet and are designed to filter malicious Attack traffic and pass-through legitimate traffic in order to Mitigate the potential disruptions caused by an Attack.

"On-Demand" refers to an option for DDoS Mitigation Direct, DDoS Mitigation Internet Direct Service or DDoS Mitigation GRE Service that diverts Customer's inbound internet traffic through the Mitigation Infrastructure using BGP networking only when Customer traffic is under Attack or suspected of being under Attack.

"Order" which may also be referred to as "Service Order" means a service order request submitted on a form issued by Lumen and signed or agreed by Customer that includes the type and details of the specific Services ordered by Customer. A Service Order will also mean the online activation of Services including submitting a request within the Portal.

"Portal" may refer to either the DDoS specific Portal where Customer will have access to see traffic monitoring, alerting and Mitigation or the general Lumen Portal where Customer may view Service inventory and Service tickets.

"Regularly Scheduled Maintenance" means any scheduled maintenance performed to the Mitigation Infrastructure. Regularly Scheduled Maintenance will not normally result in Service interruption. If Regularly Scheduled Maintenance requires an interruption, Lumen will: (a) provide Customer seven (7) days' prior written notice, (b) work with Customer to minimize such interruptions, (c) use commercially reasonable efforts to perform such maintenance between midnight and 6:00 a.m. local time where the Mitigation Infrastructure is located on which such maintenance is performed and (d) work with Customer to remove Always-On Customer traffic from the Mitigation Infrastructure during such maintenance to avoid interruption. Emergency maintenance may be performed on less or no notice.

"Resource Public Key Infrastructure" or "RPKI" is a specialized public key infrastructure standard, adopted by most internet service providers (ISPs), that was designed and developed to provide a secure means of peer-to-peer IP Route announcements (BGP Protection). RPKI helps ensure that a route announcement is legitimately coming from the source AS (Autonomous System) and that it was registered with the Route Registry.

"Service Guide" (or "SG") means the product-specific Service guide that includes technical descriptions which Lumen may modify from time to time, effective upon posting at: https://www.lumen.com/en-us/about/legal/business-customer-terms-conditions.html.

"Service Validation" means the process by which the DDoS Mitigation Service is confirmed as available as a part of the provisioning process enabling Lumen to obtain a profile of Customer's traffic. Customer will coordinate to schedule Service Validation when contacted by Lumen to do so. Service Validation is conducted over two (2) windows during which traffic is routed through the Mitigation Infrastructure as follows: (a) an initial 2 hour "test" window, and (b) a 24-hour validation window. Service Validation must be completed for all or a subset of protected Class C subnet prior to routing traffic through the Mitigation Infrastructure.

"Suspension" means Lumen's suspension of the DDoS Mitigation Service to Customer as permitted by this Service Schedule or as otherwise allowed under the Agreement.

"Third Party Software or Services" means those designated services where Customer must agree to the terms required by the vendor that form the binding agreement between the applicable vendor and Customer. For all such designated services, Lumen is not responsible or liable for the Services, including the performance of or failure to perform of the services.