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 or Lumen® DDoS Hyper℠ ("Service") 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. DDoS Mitigation Service orderable online via self-serve may be referred to as "Lumen® DDoS Hyper℠" or "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 the Service Schedule and then the Agreement.

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. The Service is available on Customer's Internet services as described in this Service Schedule. The Order will specify the type of DDoS Mitigation Services and whether those Services are Always-On or On-Demand, as applicable. DDoS Mitigation Service is available in 4 cloud-based options that Customer will select and that will be identified in the Order: (i) Direct Service, (ii) DDoS Mitigation Internet Direct Service, or (iii) GRE Service. Not all Services and features are available in all regions or countries and are subject to availability. An Order is either a form signed by Customer or a form accepted online. Not all available features are orderable via self-serve.

The 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 a monthly recurring charge. 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 under this Service Schedule, including but not limited to, installation, detection, and DDoS Mitigation Services, 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 (e.g. IPVPN Service) are subject to separate Service Schedules.

If Customer orders DDoS Mitigation Services to connect Customer's equipment managed by Lumen (regardless of equipment ownership), Customer expressly grants Lumen permission to make configuration changes to any Customer equipment managed by Lumen for DDoS Mitigation Service activation and ongoing maintenance.

2.1 Direct Service. Direct Service is activated by BGP route advertisement, with logical private line connections over IPVPN/EVPL between the Mitigation Infrastructure and Customer's border router(s). BGP routing protocol is used to communicate network advertisements from Customer to the Mitigation Infrastructure enabling inbound traffic to route through the Mitigation Infrastructure during an Attack or threatened Attack.

2.2 Internet Direct Service. Internet Direct Service is activated by BGP route advertisement delivering Mitigated traffic from the Mitigation Infrastructure to Customer's border router(s) via a shared VLAN that also delivers the Internet traffic or a separate VLAN on a Lumen provided Internet connectivity. BGP routing protocol is used to communicate network advertisements from Customer to the Mitigation Infrastructure enabling inbound traffic to route through the Mitigation Infrastructure during an Attack or threatened Attack.

2.3 GRE Service. GRE Service is activated by BGP route advertisement and is based upon the GRE protocol with virtual tunnel connections constructed to Customer's border router(s). BGP routing protocol is used to communicate network advertisements from Customer to the Mitigation Infrastructure, enabling inbound traffic to route through the Mitigation Infrastructure during an Attack or threatened Attack. Customers directly connected to the Lumen AS IP network can advertise a /32 subnet for IPv4 or /128 subnet for IPv6. Non-Lumen IP customers must advertise a /24 subnet for IPv4 and a /48 subnet for IPv6 as a minimum.

2.4 Routing under either the Direct Service, Internet Direct Service, or the GRE Service is asymmetric, with outgoing traffic from Customer to the Internet being forwarded as normal to Customer's Internet Service Provider, without passing through Mitigation Infrastructure.

2.5 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.

2.6 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.

2.7 Log Streaming Service. For the optional Log Streaming feature, Customer acknowledges that Log Streaming must be setup over an encrypted session. This Log Streaming feature requires Customer to provide Lumen with a digital SSL certificate to be loaded onto the Log Streaming platform in order for traffic to be sent over an encrypted session. Customer is responsible for configuring its SIEM (Security Information and Event management) platform and network environment to allow, accept and store logs and/or security events transmitted by Lumen. The Log Streaming service feature delivers Event notifications for up to 2 Customer provided SIEM or IP addresses. Customer acknowledges that Event notifications sent to the SIEM are delivered over the Internet and delivery may fail due to Internet connectivity issues outside of Lumen's control. Customer, and not Lumen, is responsible for storage of the logs received; however, Lumen has the ability to buffer logs if needed for up to 14 days. Customer acknowledges and agrees that Log Streaming is provided "as-is" and "as available".

2.8 Monitoring. Monitoring options for the Service are designed to provide proactive detection of DDoS Events ("Attack Monitoring Services"). Attack Monitoring Services are available as described below:

(a) Flow Based Monitoring ("FBM") provides 24x7 monitoring and alerts for large flood-based Attacks: (1) from Customer owned and managed equipment; or (2) from Lumen provided and managed equipment installed on Customer's premise, or (3) with Lumen Internet Services that choose monitoring from Lumen provider edge routers. FBM Service requires a reliable feed of netflow sampling and SNMP specific to the Customer's traffic. To the extent Customer purchases the FBM Service with the On-Demand Service, Lumen will proactively notify Customer about DDoS Mitigation system generated alarms that Lumen detects are caused by DDoS Attacks. For Attacks that are not detected by the DDoS Mtigation system, Customer must contact the SOC to initiate Mitigation. For option 1 and 2 above, there will be an MRC and an NRC for each piece of equipment when monitoring occurs from the Customer premise. For option 3 above, an MRC and an NRC for each logical circuit when monitoring occurs from Lumen provider edge routers directly from which the FBM Service collects netflow sampling.

If Customer purchases FBM and also procures from Lumen Internet connectivity and Lumen is the only provider who provides Customer Internet connectivity, Customer has the option to pre-authorize Lumen to configure systems to automatically initiate Mitigation for each attack detected by FBM. If Customer selects the auto-mitigate option, Customer must provide Lumen written notice via a change ticket in Control Center of its pre-authorized permission to begin Mitigation. Customer may later withdraw pre-authorized permission via a change ticket. Change tickets require 24 hours advance notice.

(b) Application Monitoring and Mitigation ("AMM Cloud Signaling") is hardware based DDoS detection and Mitigation, utilizing an equipment manufacturer, model, embedded software code/version approved by Lumen ("Customer CPE"), and implemented at the Customer premises to monitor the Customer's perimeter network traffic and issues alerts for layer 7 or "application layer" Attacks. AMM Cloud Signaling Service includes Lumen provided hardware that is installed on the Customer premises. Customer must be able to provide Cloud Signaling from Customer CPE to Lumen's Cloud Signaling endpoint and Customer is responsible for technical support, service and maintenance of the Customer CPE. Customer will have full administrative access to the Customer CPE and Lumen will have no access to the Customer CPE. There will be an MRC and an NRC for each Customer CPE utilizing the AMM Cloud Signaling Service.

Notwithstanding the foregoing, Lumen reserves the right at any time to: (i) change or supplement the monitoring tools and the Mitigation techniques (including but not limited to modifying the Mitigation Infrastructure); (ii) increase or decrease the monitoring tools' sensitivity to anomalous IP traffic patterns; and (iii) modify the definition of anomalous IP traffic patterns that may indicate an Attack.

2.9 Professional Security Services Assistance.

(a) PSSA is performed remotely by English speaking Lumen personnel (i.e. Lumen employees or contractors) located in the United States between the hours of 9:00 A.M. and 5:00 P.M. local time within the continental United States, Monday through Friday, and excluding United Sates statutory holidays and any additional holidays that Lumen grants to its employees, a list of which can be provided to Customer prior to the commencement of the Services upon request. If the Customer requests performance of any Service outside of such hours (non-standard hours), Customer will be responsible for any additional costs incurred as a result, as may be legally required (including without limitation any overtime pay). Lumen will determine the personnel assigned to perform the Service. No SLA applies to the PSSA services.

(b) Performance of Services by Lumen personnel is not intended to modify or change the status of such resource to that of any employee of Customer.

(c) The specific services that are desired by the Customer from the list attached as Exhibit A will be determined and mutually agreed upon during the kick-off call.

2.10 Rapid Threat Defense.

Rapid Threat Defense is an automated threat detection and response capability designed to detect and block bots based on identified behavior and confidence by Lumen's proprietary research labs ("Black Lotus Labs"). When bots are discovered that meet or exceed the confidence level, these identified bots are automatically deployed to the DDoS Mitigation Service to be used as countermeasures during

an active DDoS Attack. 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 can view automated actions via DDoS Mitigation Service Portal.

2.11 Service Level Agreements ("Service Levels") and Associated Remedies.

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 in Sections A - C below apply to the Mitigation aspect of Service. Service Levels do not apply to Excused Outages, or periods of Special Unavailability, 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 such 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 such Mitigation Infrastructure (*i.e.,* the Customer cannot pass traffic through the Mitigation Infrastructure) for more than 60 consecutive seconds. In the event 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*

*Service Credits is based on the MRC associated with the affected Service at the affected location. Per day calcuation 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 2.11 (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) and as Customer's sole remedy for any non-performance of the Service, 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 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) 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 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 Attack Mitigation requires a subscription to the Web Application Firewall and BOT Management (WAF/BOT) service which is purchased separately.

In the event the TTM SLA is not achieved, 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*

*Service Credit is based on the MRC associated with the affected Service at the affected location. Per day calcuation 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 Auto-Mitigation option or Always-On and the SOC does not have to call Customer 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) 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 applicable FBM Service or AMM Cloud Signaling Service or 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 only apply for the Mitigation aspect of the Service provided pursuant to an MRC, and will not apply to any other DDoS Mitigation Service, including, without limitation, 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. Customer will be billed monthly in advance based on a fixed rate for Mitigation up to a predefined bandwidth level. The manner of billing selected will be set forth in the Order. Fixed rate charges for DDoS Mitigation Service consist of 2 components: (a) a non-recurring charge ("NRC", "One Time Charges", or similar references") and (b) a monthly recurring charge ("MRC", "Monthly Charge", or similar references). The Service Commencement Date begins upon issuance of a Connection Notice. The Connection Notice will be issued on the first to occur of: (i) successful completion of Service Validation or (ii) five (5) business days after Lumen notifies Customer that it has provisioned all components of the Service that Lumen can provision without Customer's assistance. If there are multiple locations, billing will begin with the Service Commencement Date for the initial location (unless other locations are not available due to the fault of Lumen). Special terms may be available for a DR Site as agreed to in an Order or Addendum to the Order. For PSSA, MRC is billed in advance at the rates identified in the applicable Order. 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.

Customer may seek expedited "turn-up" of Service for an additional one-time charge ("Expedited Service"). Customer acknowleges and agrees that accepting the Expedited Services means acceptance of the DDoS Services for the Service Term specified in the Order and cooperating with Lumen to ensure the DDoS 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. Lumen reserves the right to suspend Expedited Service and the other DDoS Mitigation Services at any time if Customer fails to satisfy credit requirements which may be imposed after the completion of a credit review.

3.2 IP Addresses. If Lumen assigns to Customer an IP address as part of the provision of Service, the IP address will revert to Lumen after termination of the applicable Order for any reason whatsoever, and Customer will cease using the IP address. At any time after termination, Lumen 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, indemnify and hold Lumen harmless from any claim, demand or action arising in connection with a breach of the foregoing warranty.

3.3 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 and should be authorized to consent to make or direct changes to the Customer's security infrastructure or architecture, as applicable. Customer must provide Lumen with advance notice of at least five (5) business days of any network topology or system changes that may affect the Service or the effectiveness of the DDoS Mitigation system policy. For changes that are Service or price impacting, changes must be agreed to in a new Order before the change will go into effect. Lumen may not be able to provide the Service if Customer's point of contact information is out of date or inaccurate or if Customer performs system changes without prior notification to Lumen. Failure to notify Lumen of system changes may result in 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.

3.4 Customer must promptly notify Lumen if it believes it is under Attack and provide Lumen with reasonable assistance to reroute the IP traffic to the Mitigation Infrastructure in order for the Service to function properly.

3.5 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.

3.6 For the Direct Service, Customer must procure from Lumen connectivity between the Lumen network and the Customer premises or data centers (border routers) per the following criteria: (i) the demarcation point is the physical network port of the Mitigation Infrastructure, (ii) the connectivity must consist of at least one (1) IPVPN circuit directly to the port on the Mitigation Infrastructure from each of Customer's premises or data centers, and (iii) any Ethernet circuit must support 802.1Q. Provisioning begins upon confirmation of IPVPN circuit availability. Lumen may suspend Direct Services if Lumen detects that any Customer provided equipment is causing interference with the Lumen network or other customers. Any IPVPN circuit provided by Lumen will be subject to service levels as set forth in Lumen's standard service schedule for such service or as otherwise agreed in writing by Customer and Lumen.

3.7 For the Internet Direct Service, Customer must procure from Lumen connectivity between the Lumen network and the Customer presmises or data centers (border routers) per the following criteria: (i) the demarcation point is the physical network port of the Mitigation Infrastructure, (ii) the connectivity must consist of at least one (1) Lumen Internet Service circuit capable of connecting to the port on the Mitigation Infrastructure from each of Customer's premises or data centers (subject to availability), and (iii) any Ethernet circuit must support 802.1Q for delivery of Internet and scrubbed traffic on a shared VLAN that also delivers the Internet traffic or two (2) separate VLANs. Provisioning begins upon confirmation of Lumen Internet Service circuit availability. Lumen may suspend Internet Direct Services if Lumen detects that any Customer provided equipment is causing interference with the Lumen network or other customers. Any Lumen Internet Service circuit provided by Lumen will be subject to service levels as set forth in Lumen's standard service schedule for such service or as otherwise agreed in writing by Customer and Lumen.

3.8 Notification Responsibilities. Customer must provide Lumen with of 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; and (v) immediate notice if Customer believes it is under a DDoS Attack (vi) immediate notice related to any changes to Customer's contact information, including email.

3.9 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.

3.10 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.

3.11 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.

3.12 In relation to Professional Security Services Assistance, Customer agrees to complete an upfront questionnaire that gathers necessary context for performance of the PSSA service including but not limited to: (i) Business context being protected by DDoS Service; (ii) Identify any applicable compliance standards that apply to their business; (iii) Identify any existing DDoS concerns; (iv) identify any business changes that may have near-term impacts on traffic patterns impacting DDoS protection. In addition, Customer agrees to (i) provide a point of contact to coordinate the service activities; (ii) provide Lumen with timely responses to inquiries around providing the service; (iii) timely participation in phone call(s) to discuss conditions or questions regarding any activities; (iv) specifically identify and provide Lumen with access to all relevant Customer-controlled information, resources and locations required to perform and/or complete the Services.

3.13 Installation/Setup. Customer will cooperate with Lumen by providing Lumen with all information concerning the Service reasonably requested by Lumen and providing the 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.

3.14 Lumen Provided Software. (a) If any third-party software, including any corresponding documentation, is provided to Customer by Lumen in connection with the Service, Customer agrees to use third party software strictly in accordance with all applicable licensing terms and conditions including any click to accept terms required as part of the download/install process. Customer will defend, indemnify and hold Lumen harmless from any claim, demand or action arising in connection with Customer's failure to comply with the third party terms or use of third party software in a manner not authorized by this Schedule; and (b) 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.

3.15 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.

3.16 Change Request. Customer ordering DDoS Mitigation Service must request non-price impacting Service changes by opening a ticket or by contacting the SOC. Customer 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℠ can make non-price impacting Service changes or service design changes that are price impacting, but they require a change order via the online self-service interface.

3.17 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.

3.18 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 of the Attack(s) on Customer's IP address will be reduced.

3.19 Portal Use. If Lumen provides Customer with Portal access in connection with the Service, Customer will use access solely as 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. The 2FA tokens will be disabled for accounts that have not been active in more than six (6) months requiring such users to request new tokens if they wish to

reestablish access. In addition, as ar 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 or any employee of Lumen develops or creates any intellectual property as part of DDoS Services ("DDoS Intellectual Property"), that DDoS Intellectual Property will be, and remain, the exclusive property of Lumen, 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 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 a 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 Personal Data. Customer and Lumen acknowledge that it may be necessary to provide the other party with personal data or to access personal data of the other party as necessary for the performance of each party's obligations under the Agreement and/or this Service Schedule, including, but not limited to and where applicable, employees' and authorized representatives' names, business contact information, technical or operational data (such as online identifiers), credentials to access Portals and other platforms made available by one party to the other and similar personal data. The parties acknowledge and agree that each is a controller with respect to any such personal data exchanged under the Agreement and/or this Service Schedule, and any such personal data is provided on a controller-to-controller basis. Any personal data exchanged in accordance with this Section will be limited to the extent necessary for the parties to perform their obligations or exercise their rights under the Agreement or this Service Schedule. As used in this Service Schedule, the terms "personal data," "processing," "processor" and "controller" will have the meanings ascribed to them in applicable data protection laws, including, without limitation, the European Union General Data Protection Regulation (Regulation (EU) 2016/679). Each party will be independently and separately responsible for complying with its obligations as a controller under applicable data protection laws in its capacity as a data controller with respect to the personal data it provides to the other party and/or receives from the other party. Unless otherwise set forth in the Agreement, Lumen personnel will not access or attempt to access personal data that is processed via the operation of the Service. Processing is typically carried out at machine-level and Lumen will not retain any copies of data longer than necessary to perform the applicable Service or perform under the Agreement. To the extent legally required, Customer and Lumen will enter into separate written agreements required to comply with laws governing the relationship between a controller and processor with respect to the processing of personal data described in this Section, including, without limitation, any agreements required to facilitate necessary cross-border personal data transfers. Customer will be responsible for notifying Lumen whether such written agreements are required based on the nature of the data being processed.

4.3 Additional Disclaimer of Warranty; Liability.

4.3.1 Customer acknowledges the Services endeavor to Mitigate security Events, but such Events, even if determined to be Attacks, may not be mitigated entirely or rendered harmless. Customer further acknowledges that it should consider any particular 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 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.

Lumen may temporarily suspend any Service immediately in the event 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 in the event Lumen or an applicable vendor or subcontractor cannot maintain any required regulatory approvals, despite its reasonable efforts to do so. In the event of any expiration or termination of any Service, Customer's access to the applicable Services will end and the Services do not include assisting Customer with any transition to an alternative provider.

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. Customer understands that DDoS may result in disruptions of and/or damage to end-user Customers' 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 DDoS 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 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.

"Clean (Post-Mitigation) Traffic Capacity" means the level of traffic using standard DDoS Mitigation Service as identified on the Order that is returned to the Customer "clean" following the Mitigation process.

"Cloud Signaling" means the process by which Application Monitoring and Mitigation Service hardware deployed at the Customer premises utilizes automated monitoring tools to detect anomalies in IP traffic patterns and signals a potential Attack to Lumen's Mitigation Infrastructure.

"Customer Disaster Recovery Site" ("DR Site") means an alternative backup site that is used when a primary location becomes unusable due to failure or disaster. Customer will not use the DDoS Mitigation Service with production traffic at the DR Site except when use of the Customer primary site fails.

"Customer-Initiated Mitigation" is an optional feature for Always-On DDoS Mitigation Direct Service, Internet Direct Service or GRE Service that allows customers to initiate mitigation via BGP route announcements to Lumen rather than calling the Lumen Security Operations Center ("SOC"). Customer-Initiated Mitigation is equivalent to Customer approval to route traffic to the Mitigation Infrastructure for purposes of the TTM SLA. Customer-Initiated Mitigation is subject to Lumen availability based on its network configuration. If available, Customer must dynamically advertise the preferred prefixes into the clean return tunnels and the advertised prefixes automatically propagate from the Mitigation Infrastructure to the Internet and the Service automatically begins scrubbing the advertised traffic. The maximum number of prefixes that can be advertised via Customer-Initiated Mitigation is subject to technical constraints. Customer may elect this feature at the time of provisioning or after the Service is turned up via a ticket or by submitting to the SOC.

"DDoS Hyper" or "Lumen® DDoS Hyper℠" means DDoS Mitigation Service orderable online via self-serve experience. Lumen® DDoS Hyper℠ includes a subset of service capabilities available within DDoS Mitigation Service.

"DDoS Mitigation Direct Service" or "Direct Service" or "IP VPN Direct Service" means DDoS Mitigation implemented using BGP route advertisements as a mechanism to re-route legitimate and Attack traffic through the Mitigation Infrastructure. Clean traffic is routed back to the Customer data center over IPVPN/EVPL logical connections between the Mitigation Infrastructure and Customer's border router(s).

"DDoS Mitigation GRE Service" or "GRE Service" means DDoS Mitigation implemented using BGP route advertisements as a mechanism to re-route legitimate and Attack traffic through the Mitigation Infrastructure. Clean traffic is routed back to the Customer data center using a GRE tunnel.

"DDoS Mitigation Internet Direct Service" or "Internet Direct Service" means DDoS Mitigation implemented using BGP route advertisements as a mechanism to re-route legitimate and Attack traffic through the Mitigation Infrastructure. Clean traffic is delivered on a Lumen provided Internet Service circuit only back to the Customer data center over a shared VLAN logical connection that also delivers the Internet traffic or separate VLAN logical connection.

"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 of Customer, its employees, contractors or agents or its end users; (b) the failure or malfunction of equipment, applications, the public Internet, 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 improper or inaccurate network specifications provided by Customer; (i) Customer is in breach of its obligations under the Agreement or this Service Schedule; or (j) Customer failure to properly update the Route Origin Authorization ("ROA").

"Log Streaming" is an optional feature that allows customers to receive logs and Mitigation Event data to Customer's designated destination via syslog format. The Mitigation Event data is the information obtained from the Mitigation Infrastructure.

"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.

"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.

"Professional Security Services Assistance" or "PSSA" is an optional add-on feature that includes a quantity of hours per month, to be identified in the Order, of consulting, advisory and operational services by providing a designated, remote point of contact for the Customer throughout the term of the DDoS Mitigation Service. A Lumen Security Specialist will perform a variety of support tasks, as well as ongoing support and consultative activities related to the Lumen DDoS Mitigation service.

"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 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 such 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.

"Special Unavailability" means the SLA will not apply, and Customer will not be entitled to receive a credit or exercise a termination right under the SLA related to unavailability of the Service due to (a) Customer misuse; (b) network unavailability, including telecommunications failures outside of the Mitigation Infrastructure or Lumen network and outside Lumen's sphere of responsibility; (c) 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; (d) any other action or inaction by a third party not attributable to Lumen. Whether Special Unavailability is present will be determined by Lumen on the basis of available records, data and other evidence.

"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.

EXHIBIT A
For Informational Purposes Only

List of PSSA Services currently available are identified below. Lumen reserves the right to update the list of available services from time to time.

Onboarding and Activation

- Project management from ordering to activation
  - Project kick off call with Customer
  - Project status monitoring and regular status update
  - Pre-activation walk-through of environment to be protected
  - Assistance with Portal enrollment
- Custom runbook document development based on Customer's needs and delivery of the runbook to the Lumen Security Operations Center (SOC) prior to DDoS Mitigation Service being provisioned
- Portal training

Monitoring and Configuration Analysis

- Verification that all required circuits are being protected
- Reviews and policy verifications for protected IPs and networks
- DDoS incident reviews for trending including targets, methods, and frequency
- Customer historic DDoS activity reviews to determine optimal policy threshold settings for alerts and Mitigation countermeasures
- Mitigation alert policy review to verify appropriate contacts are notified
- Auto-mitigation versus manual Mitigation scenario reviews with Customer
- Mitigation zone grouping reviews with Customer for maximum Mitigation effectiveness
- DDoS Mitigation Service separation reviews, such as web, email and DNS
- Configuration improvement reviews and recommendations for optimal protection
- False positive reviews and recommended methods to limit future occurrences

Regular (quarterly, semi-annual, or annual) DDoS Service Reporting

- Written reporting containing analysis, advice and recommendations
  - DDoS attack trending summary reports
  - SOC ticket report generation and reviews with Customer with ongoing feedback provided to SOC
- Regular reviews with Customer to discuss findings and recommendations
  - Advisement of any new or additional IPs or networks that should be protected
  - Advisement of recommended changes to DDoS Mitigation settings for optimal defense against attacks
  - Mitigation countermeasure tuning recommendations to prevent impacts to production environments and minimize false positives
- Custom runbook updates based on Customer's needs, with all updates provided to SOC