DDoS MITIGATION TERMS AND CONDITIONS

In these DDoS Mitigation Terms and Conditions ("DDoS Terms and Conditions"), "you" and "your" mean the "Customer" of the Cox services defined below, and "Cox," "we," "our," and "us" means Cox or any contractor authorized by Cox to provide you with DDoS Services. BY ENROLLING IN, USING, OR APPLYING FOR DDoS SERVICES (as defined below), YOU AGREE TO THE TERMS AND CONDITIONS SET FORTH BELOW, AS WELL AS THE TERMS AND CONDITIONS TO YOUR CUSTOMER SERVICE AGREEMENT (as defined below) AND ANY ATTACHMENTS THERETO. . IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS DO NOT USE OR UTILIZE THE DDOS SERVICES AND IMMEDIATELY CALL YOUR COX SALES REPRESENTATIVE OR THE CUSTOMER SERVICE NUMBER LISTED ON YOUR COX BILL

1. SCOPE

These DDoS Terms and Conditions govern the provision of DDoS Mitigation Services ("DDoS Services") as described herein.

2. DEFINITIONS

2.1 Definitions of Base Package Options for DDoS Services.

2.1.1 "BGP Direct Premium" means the on-demand, cloud-based service which cleans or scrubs, by means of the Mitigation Platform, certain internet-based, malicious, attack traffic from the legitimate, internet-based clean traffic directed at the Customer Endpoint and which is activated by Neustar pursuant to Cox's authorization and which announces a IPv4 /24 prefix or IPv6 /48 prefix from the Mitigation Platform and which imposes no fee for Attack Incidents but is subject to other applicable fees, as expressly set forth herein. For the purpose of clarity, election of Auto-Mitigation, until or unless revoked, shall constitute standing Customer authorization to proceed.

2.1.2 "BGP Direct Standard" means the on-demand, cloud-based service which cleans or scrubs, by means of the Mitigation Platform, certain internet-based, malicious, attack traffic from the legitimate, internet-based clean traffic directed at the Customer Endpoint and which is activated by Neustar pursuant to Cox's authorization direction and which announces a IPv4 /24 prefix or IPv6 /48 prefix from the Mitigation Platform and which is subject to Mitigation Incident Fees and other applicable fees, as expressly set forth herein. For the purpose of clarity, election of Auto-Mitigation, until or unless revoked, shall constitute standing Customer authorization to proceed.

2.1.3 "BGP IP Premium"" means the on-demand, cloud-based service which cleans or scrubs, by means of the Mitigation Platform, certain internet-based, malicious, attack traffic from the legitimate internet-based, clean traffic directed at the Customer Endpoint which is activated by Neustar pursuant to Cox's authorization and which announces a IPv4 prefix size ranging from /24 through a /32 which leverages the private connection and peering that is configured between Cox and Neustar and which imposes no fee for Attack Incidents but is subject to other applicable fees, as expressly set forth herein. For the purpose of clarity, election of Auto-Mitigation, until or unless revoked, shall constitute standing Customer authorization to proceed.

2.1.4 "BGP IP Standard" means the on-demand, cloud-based service which cleans or scrubs, by means of the Mitigation Platform, certain internet-based, malicious, attack traffic from the legitimate internet-based clean traffic directed at the Customer Endpoint which is activated by Neustar pursuant to Cox's authorization and which announces an IPv4 prefix size ranging from /24 through a /32 which leverages the private connection and peering that is configured between Cox and Neustar and which is subject to Mitigation Incident Fees and other applicable fees, as expressly set forth herein. For the purpose of clarity, election of Auto-Mitigation, until or unless revoked, shall constitute standing Customer authorization to proceed.

2.2 Definitions of Fees.

2.2.1. "Clean Traffic Overage Fee" or "CTOF" means the fee, calculated on a per Mbps per Incident basis, that will apply in the event that amount of Clean Traffic during an Incident exceeds the amount of traffic for which Customer has contracted.

2.2.2. "Configuration Change Fee" or "CCF" means the fee which shall apply to any Cox or Customer-initiated changes to the Mitigation Platform configuration such as additions, deletions and updates related to IP addresses, domain names, ports and protocols. The fee shall apply to any Configuration Change which is not performed on an expedited or emergency basis or in conjunction with an upgrade.

2.2.3. "Deployment Fee" means the fee that applies for Deployment of the DDoS Services.

2.2.4. "Emergency Configuration Change Fee" or "ECCF" means the fee which shall apply in the event that, in response to a Customer request, a configuration change is requested for emergency or expedited provisioning is performed by Cox within five (5) hours of Cox's approval of Customer request. The ECCF shall apply in addition to any related Mitigation Incident Fees and other applicable fees.

2.2.5. "Mitigation Incident Fee" or "MIF" means the fee which shall be assessed in the event of a Mitigation Incident and shall apply for every period of seventy-two (72) consecutive hours or a fraction thereof.

2.2.6. "Non-Attack Incident Fee" or "NAIF" means the fee applicable to use of the DDoS Service during a Non-Attack Incident and shall apply every seventy-two (72) hours or portion thereof wherein Customer directs internet-based traffic for an Endpoint to the Mitigation Platform.

2.2.7. "Test Failover Fee" or "TFF" means the fee which shall apply in the event that, in response to Customer request, Cox performs a test of Customer traffic failing over to the Mitigation Platform. Two (2) Test Failovers per twelve (12) month term are included in standard packages. Tests must be scheduled at least forty-eight (48) hours in advance with the Cox SOC and Support teams, and are limited to 200Mbps of clean traffic unless otherwise approved by Cox.

2.3 General Definitions.

2.3.1 "/24 Prefix" means a "Class C" block of IPv4 address space which contains two hundred fifty six (256) contiguous IP addresses.

2.3.2 "/48 Prefix" means a block of IPv6 address space which contains 1,208,925,819,614,629,174,706,176 contiguous IP addresses.

2.3.3 "Additional Dynamic VIPs (20 VIP's Per Package)" means a pool of Cox-assigned IP addresses on the Mitigation Platform from which, at the initiation of mitigation, Customer is assigned a virtual IP address for use with the Mitigation Platform.

2.3.4 "Additional GRE Connection/Location" means a router endpoint to terminate GRE (Generic Routing Encapsulation) tunnels connected to the Mitigation Platform. GRE tunnels are applicable to the BGP Direct service type with either the Standard or Premium mitigation option. Standard base packages include 1 GRE Connection/Location.

2.3.5 "Appliance" means the equipment provided by Cox to Customer for the purpose of mitigating Attacks.

2.3.6 "Attack" or "Attack Incident" shall mean an event in which malicious traffic (e.g. DDoS), is directed at an Endpoint which is on the Mitigation Platform. The determination as to whether traffic is Attack traffic shall be determined solely by Cox.

2.3.7 "Auto-Mitigation" means Customer's blanket authorization that allows Cox to proactively mitigate Incidents.

2.3.8 "Clean Traffic" shall mean the ninety-fifth (95th) percentile peak Mbps of legitimate (non-malicious), traffic going in to or out of the Mitigation Platform, which is processed by the DDoS Service during an Incident.

2.3.9 "Customer's Service Agreement" means the document agreed to by Customer and Cox for the DDOS Service (for example, the Commercial Services Agreement or the Master Retail Services Agreement, whichever is applicable).

2.3.10 "Configuration Change" means Customer-requested changes to the Mitigation Platform configuration performed by Cox, such as additions, deletions and/or updates related to IP addresses, domain names, ports and protocols.

2.3.11 "DDoS Detection and Alerting" or "DDoS Detection & Alerting with Monitoring & Notification Only" means a service that accepts Netflow management data from Customer routers for the purpose of monitoring and alerting Customer of suspicious traffic based on parameters established during the initial Provisioning Process.

2.3.12 "DDoS Detection and Alerting Deployment" means a service that includes recommendations regarding the setup of DDoS Detection and Alerting Services and auto-mitigation, if applicable.

2.3.13 "DDoS Detection & Alerting with Monitoring, Notification & Auto-Mitigation" means a service that accepts Netflow management data from Customer routers for the purpose of monitoring and alerting where Cox is authorized to perform Auto-Mitigation for the impacted prefixes. In order to have Auto-Mitigation occur, Customer must announce a lesser portion of the Prefix (a /23 or less for IPv4 & a /47 or less for IPv6), Cox would then announce the larger, more specific prefix (/24 or /48).

2.3.14 "DDoS Mitigation Platform" or "Platform" means the Cox network to which Customer must direct traffic for an Endpoint in order to access the cloud-based DDoS Services.

2.3.15 "DDoS Services" means individually and collectively, those services set forth in Section 2.1 above.

2.3.16 "Deployment" means initial setup of the DDoS Service for Customer by Cox and an assigned resource through the duration of onboarding, including kick off call, tracking/ status updates, testing, and consultation and closing call.

2.3.17 "Deployment Date" means the date when the DDoS Service is installed.

2.3.18 "Endpoint(s)" means that part of Customer's infrastructure for which Customer has activated the DDoS Services by directing traffic to the Endpoint onto the Mitigation Platform.

2.3.19 "HTTPS Packet Inspection" means the service in which Customer provides Cox with a copy of the SSL certification of an encrypted website.

2.3.20 "Incident" means an event wherein Customer has directed internet-based traffic for an Endpoint to the Mitigation Platform and shall include both Attack Incidents and Non-Attack Incidents.

2.3.21 "Layer 3 of the OSI Model" or "Layer 3" means the network or 3rd layer provides the functional and procedural means of transferring variable length data sequences (datagrams) from one node to another connected to the same network. It translates logical network address into physical machine address. A network is a medium to which many nodes can be connected, on which every node has an address and which permits nodes connected to it to transfer messages to

other nodes connected to it by merely providing the content of a message and the address of the destination node and letting the network find the way to deliver ("route") the message to the destination node. In addition to message routing, the network may (or may not) implement message delivery by splitting the message into several fragments, delivering each fragment by a separate route and reassembling the fragments, report delivery errors, etc. Datagram delivery at the network layer is not guaranteed to be reliable.

2.3.22 "Layer 4 of the OSI Model" or "Layer 4" means the transport or 4th layer provides the functional and procedural means of transferring variable-length data sequences from a source to a destination host via one or more networks, while maintaining the quality of service functions. An example of a transport-layer protocol in the standard Internet stack is Transmission Control Protocol (TCP), usually built on top of the Internet Protocol (IP). The transport layer controls the reliability of a given link through flow control, segmentation/desegmentation, and error control. Some protocols are state and connection-oriented. This means that the transport layer can keep track of the segments and retransmit those that fail. The transport layer also provides the acknowledgement of the successful data transmission and sends the next data if no errors occurred. The transport layer creates packets out of the message received from the application layer.

2.3.23 "Layer 7 of the OSI Model" or "Layer 7" means the application or 7th layer is the OSI layer closest to the end user, which means both the OSI application layer and the user interact directly with the software application. This layer interacts with software applications that implement a communicating component. Such application programs fall outside the scope of the OSI model. Application-layer functions typically include identifying communication partners, determining resource availability, and synchronizing communication. Some examples of application-layer implementations include web browsers, file transfer programs and mail programs.

2.3.24 "Level 1 Notification" or "Level 1" (Monitoring & Notification) shall means an event, which Cox has determined represents a high likelihood of being a DDoS Attack on the monitored Endpoint(s).

2.3.25 "Level 2 Notification" or "Level 3" (Monitoring & Notification) means that an event, which Cox has determined represents a potential traffic anomaly on the monitored Endpoints(s).

2.3.26 "Level 3 Notification" or "Level 3" (Monitoring & Notification) mean that an event, which Cox has determined represents a potential traffic anomaly on the monitored Endpoints(s).

2.3.27 "Location" means Customer router endpoint to terminate GRE (Generic Routing Encapsulation) tunnels connected to the Mitigation Platform.

2.3.28 "Mbps" means Megabit per second.

2.3.29 "Mitigation Incident" means either (a) the event commencing when Cox announces the requested prefix(es) out of the Mitigation Platform and ceases when Customer contacts Cox pursuant to the current Cox policies and directs Cox to cease such announcement(s) or (b) an event where more than twenty-five (25) kilobits per second ("Kbps") of Customer traffic flows through the Mitigation Platform.

2.3.30 "Mitigation Period" means the forty-eight (48) hour period immediately preceding or following an Attack Incident wherein Customer shall not be charged the Non-Attack Incident Fee.

2.3.31 "Mitigation Platform" means the Cox network to which Customer must direct traffic for an Endpoint in order to access the cloud-based DDoS Services.

2.3.32 "Non-Attack Incident" shall mean an event immediately following the Mitigation Period in which Customer has directed internet-based traffic for an Endpoint to the Mitigation Platform and there has been no Attack traffic for a period of seventy-two (72) hours.

2.3.33 "Performance Alerting" means a service that conducts external, real-browser monitoring and then if an event is detected, alerts Customer by email if their infrastructure possibly warrants administrative attention related to internet degradation or unavailability of their website.

2.3.34 "Provision" means to provision the DDoS Services by Deployment, to make a Configuration Change and/or the process related to the DDoS Detection and Alerting and/or Performance Monitoring services.

2.3.35 "Provisioning Call" means discussion(s) between Customer and Cox after receipt of a Provisioning Document or Configuration Change to address matters pertaining to the provisioning and Deployment.

2.3.36 "Provisioning Document" means the agreed upon set of documents related to the initial Provision of DDoS Services or related to the DDoS Detection and Alerting and/or Performance Monitoring services.

2.3.37 "Provisioning Process" means Cox's process for Deployment, Configuration Changes and/or the process related to the receipt and acceptance of a Provisioning Document

and/or Configuration Change; completion of Provisioning Call(s).

2.3.38 "Service Level" or "SLA" means the service level applicable to the relevant DDOS Service as set out in Section 8.1 through 8.7 below.

2.3.39 "Service Outage" means a failure of the DDOS Service to meet the applicable Service Level for availability of the Mitigation Platform and Customer web portal.

2.3.40 "Test Failover" means an event in which Customer sends up to 200 Mbps of traffic to the Mitigation Platform over a twenty-four (24) hour period for the purpose of testing connectivity between Endpoints and the Mitigation Platform.

2.3.41 "Traffic Scrubbing" means the DDoS Mitigation Platform process and action of analyzing incoming packets and discarding DDoS Attack packets and returning to Customer the clean packet traffic.

2.4 Definitions Applicable to Optional Services.

2.4.1 "Redundant GRE Connections (Pair)" means a redundant GRE configuration involves creating a redundant persistent GRE tunnel for Customer on Cox's Mitigation scrubbing center edge router. This allows traffic to automatically transition to the secondary connection if the primary connection fails. Once the primary connection is restored, traffic is automatically transition back to the primary connection. This configuration enables Customer to pre-designate a failover GRE endpoint for given prefixes, which could include multiple edge routers or a backup site. Customer is responsible to preconfigure a GRE interface identical to the primary for designated backup destination. Customer must complete acceptance testing with Cox.

2.4.2 "GRE Load Balancing GRE" means Load Balancing that allows for active load sharing of inbound traffic across multiple GRE tunnels for the same destination prefix. This functionality is enabled via persistent GRE tunnels between Mitigation edge routers and Customer edge routers. If connections fail, traffic will automatically be redistributed across remaining connections. When connection is restored, it is automatically returned to service and load is redistributed. This feature does not alter the standard BGP Redirect Customer-side router configuration as no BGP sessions are necessary between Cox and Customer. Underlying equal static routes allow for route determination. GRE keep-alives allow for the detection of tunnel failures and enable GRE failover.

2.4.3 "BGP /24 Mitigation Split" allows Customers to split a /24 (IPv4) or /48 (IPv6) into smaller subnets and send scrubbed traffic destined for that segment to a different destination end point. Customer premise router configuration is the same as a standard BGP Redirect Customer and clean traffic is statically routed to Customer over a GRE tunnel. Subnetting is limited to /26 (/46 if IPv6). Limiting each prefix split to 4.

2.4.4 "Multi-Hop BGP (Customer Router Auto Withdrawal)" means Multi-hop BGP is configured as a BGP session between Cox's scrubbing center edge routers and Customer edge router. A GRE tunnel is established on demand as per the standard BGP Redirect configuration, but the BGP session is established outside that GRE tunnel. Cox uses an established BGP community to dampen/withdraw Customer-announced route for the prefix to be mitigated to allow a Cox announcement of that prefix to be the preferred/only route for the prefix to be mitigated.

2.4.5 "BGP Peering over GRE" involves configuration of persistent GRE tunnel(s) and dynamic BGP session(s) between the cloud edge router and Customer edge router. GRE can be setup as either static or dynamic and can be used with GRE Failover or Load Balancing options. This enables tunnel load sharing between multiple GRE Customer destinations for the same prefix. This configuration option also allows Customer to announce and withdraw (to end mitigation) prefixes directly with Cox.

2.4.6 "BGP Peering over Direct Connection" means Customer direct connection with Cox via cross connect (x-conn) at one of the Mitigation scrubbing centers due to high clean traffic volumes and the potential for packet loss via GRE tunnels (>2Gbps) over the open internet. BGP peering directly between a Mitigation edge router and Customer edge router via x-conn enables Customer to inject and withdraw (to end redirection post-mitigation) routes directly with Mitigation for prefixes that have been pre-established and configured with Cox during provisioning or a change request. Configuration of BGP session(s) on Customer premise equipment is the responsibility of Customer, but Cox will perform testing including a cutover to ensure proper functionality during provisioning.

3. BILLING

3.1 Cox will begin billing for DDOS Services on the Deployment Date.

4. CUSTOMER OBLIGATIONS FOR SERVICES

4.1 General. Customer shall not use, or allow use of, the DDoS Services in any of the following manners ("Abuses"): (a) Use of the DDoS Services in an unlawful manner or for an unlawful purpose, including display of unlawful content; (b) Use of the DDoS Services in a manner that, in Cox's discretion, directly or indirectly produces or threatens to produce a material negative effect on the Cox's network or that materially interferes with the use of the DDoS Services or Cox network by other Customers or authorized users, including, without limitation, overloading servers or causing portions of Cox's network to be blocked; and (c) Altering any aspect of the DDoS Service where such is not authorized by Cox.

4.2 Provisioning. Customer is required to fully and accurately complete a Provisioning Document and provide all information and authorizations requested during the Provisioning Process (collectively "Provisioning Information")

prior to the initiation of the DDoS Service. Customer further acknowledges that such steps are critical in order for DDoS Services to be deployed. In the event that Customer has failed and/or refused to submit a Provisioning Document or participate in a Provisioning call and so long as Cox has contacted Customer in an effort to complete the Provisioning Process, Cox may thereafter terminate any agreement it has with Customer to provide DDoS Services by providing written notice to Customer, provided that Customer shall pay all one-time fees and all monthly recurring fees associated with the DDoS Service through the effective date of termination, and further provided that Customer shall owe no less than one (1) month of monthly recurring fees (and all one-time fees) in the event such termination occurs less than one (1) month after the delivery of the Provisioning Document to Customer. Any termination shall be deemed to be effective upon receipt of notice from Cox.

4.3 Compliance with DDoS Service Procedures & Uses. In addition to the above Customer agrees to: (a) provide all information requested by and pursuant to the Provisioning Process for each Endpoint prior to activation of the DDoS Services with respect to that Endpoint; (b) for the BGP Service, provide a BGP and GRE capable device and properly configure such device; (c) use the Appliance(s) solely for the DDoS Services and shall make no changes to the Appliance; (d) provide the necessary assistance to Cox in order to effect redirection for an Endpoint to the Mitigation Platform; (e) grant Cox with: (i) information on the Endpoints as requested by Cox and such other information that Cox requires in order to provide the DDoS Services; and (ii) access to the Endpoints in order to perform the DDoS Services; (f) for the BGP Service, authorize redirection of the internet traffic for the Endpoint from the Appliance(s) to the Mitigation Platform via the Provisioning Process; (g) and hereby does expressly consent to the repeated filtering of traffic to the Endpoint; (h) and hereby grants Cox, for the Term, a non-exclusive, non-transferable, and royalty-free license to access the Endpoint and the internet traffic flowing thereto and any applications contained therein for the sole purpose of performing the DDoS Services (i) be solely responsible for authorizing Cox to direct of all internet traffic for an Endpoint by following Cox's procedures then in effect under the Provisioning Process (which may include, by way of example, contacting support and having Cox announce or cease announcing the requested IPv4 or IPv6 prefixes; and (j) route all traffic for an Endpoint to Cox during an Attack Incident. For the sake of clarity: (a) Customer acknowledges that its failure to authorize redirection of traffic for an Endpoint away from the Mitigation Platform once Attack Traffic has ceased shall cause Customer to incur Non-Attack Incident Fees and, if applicable, Clean Traffic Overage Fees; (b) Customer acknowledges that the BGP Service is an on-demand service for use during Attack Incidents only and is not meant to be used as an always-on service during periods when an Attack is not occurring; and (c) Customer is solely responsible for support and maintenance of the Appliance(s). Cox shall not be liable for any failure to meet an SLA or to perform the DDoS Services where such inability arises from failure or non-performance of the Appliance(s) or the inability of Cox to connect to the Appliance(s).

4.4 Customer Breach. Customer shall notify Cox of any breach of security of which it becomes aware, and which may have an impact on Cox's network or provisioning of the DDoS Services.

5. LANGUAGE

5.1 English Language. Where applicable, all obligations of each Party, including, without limitation, delivery of the Services, interfaces, support obligations or requests, notices shall be performed in English, and all interaction, whether with Customer or with Cox, shall be conducted using English.

6. REFUSAL OF SERVICES

6.1 Refusal of Services. Cox may, in its commercially reasonable discretion, refuse to provide DDoS Services to any party engaged in the adult, gaming or gambling industries or any party engaged in offshore activities which are illegal under US law, or any party engaged in illegal activities or any party which is operating or located in embargoed countries.

7. SERVICE LEVELS & REMEDIES

DDoS Service Levels. Cox shall endeavor to meet the SLAs set forth below. Customer's sole and exclusive remedy and Cox's sole and exclusive obligation for a breach of the SLA obligation will be the remedies set forth in the SLA. For the sake of clarity, no SLAs shall apply to Appliances or any hardware or software contained therein.

7.1 Deployment. Deployment shall be performed within seventy-two (72) hours for completion of the Provisioning Process. Deployment for traffic transfer option for BGP shall be performed within one hundred and twenty (120) hours of the events set forth above.

7.2 Configuration Changes. Configuration Changes shall be performed within seventy-two (72) hours of the following events: (i) for DNS Redirection based Services, completion of the provisioning call and acceptance by Cox of the configuration change submission; and (ii) for BGP Redirection based Services, completion of the Provisioning Process and acceptance by Cox of the configuration change submission.

7.3 Emergency Configuration Changes. Emergency Configuration Changes shall be performed within four (4) hours of acceptance by Cox of the emergency configuration submission.

7.4 Time to Mitigate. After Deployment, Mitigation shall occur within the following periods: (i) five (5) minutes for Layer 3 and Layer 4 attacks from the time traffic is redirected to DDoS Mitigation Platform and the Platform has detected malicious traffic; and (ii) fifteen (15) minutes for Layer 7 attacks from the time traffic is redirected to the DDoS Mitigation Platform and the Platform has detected malicious traffic. Each attack vector change shall start a new Time to Mitigate. Mitigation shall mean the occurrence of Traffic Scrubbing as set forth in Section 7.5 below.

7.5 Traffic Scrubbing. Traffic Scrubbing be performed to a level of 95% clean pass-through which shall mean that the traffic shall be cleaned such that no more than five percent (5%) of dirty/malicious traffic shall be passed to an Endpoint and no less than ninety-five percent (95%) of the clean/benign traffic shall be passed to the point after which it leaves the DDoS Mitigation Platform.

7.6 DDoS Monitoring & Notification. Where the DDoS Service has been deployed, Cox shall alert Customer: (i) by phone within five (5) minutes from the time that Cox determines that there is a high likelihood of a DDoS attack on the monitored Endpoint(s); and, where applicable, (ii) by email within ten (10) minutes from time that Cox determines the legitimacy of the alert.

7.7 Performance Alerting. Where the DDoS Service has been deployed, Cox shall monitor a domain from up to four (4) global locations every five (5) minutes up to three (3) steps for a

single domain, with a one (1) minute timeout threshold which will validate a detected possible issue from three (3) locations and will alert Customer by email if their infrastructure possibly warrants administrative attention related to internet degradation or unavailability of their website

7.8 Limited Application of SLA. For the sake of clarity, the Service Levels set out in Sections 7.1 thru 7.7 shall not apply to any Appliances, hardware or software used in the provision of or related to the performance of the DDoS Services. Further, Customer's provision of information requested by Cox is hereby deemed a condition precedent to Cox's performance of its obligations hereunder.

REMEDIES.

For the avoidance of doubt, the performance of the DDoS Services and all elements related thereto are solely and exclusively governed by the Service Levels and the remedies, if any, contained in this Section 7 and shall be Customer's sole and exclusive remedy for any failure of the DDoS Services or failure of Cox in performing or delivering the DDoS Services. This shall include, but not be limited to, a failure to properly configure or route traffic, mistaken suspension of any DDoS Service, or failure to inspect packets, etc.). In some instances, a remedy may not be provided for a failure of the DDoS Services or a failure of Cox in performing the DDoS Services.

7.9 A "Credit" as used herein shall be one (1) day of Customer's monthly recurring fees for the relevant DDoS Service, pro-rated by dividing the monthly fees for that Customer by the number of days in the calendar month in which the Service Outage occurs. The maximum Credit in any given month for a given Customer shall not exceed the total Customer monthly recurring service fees for the applicable DDoS Service for that month. No one time fees, as-needed fees or non-recurring fees shall be included in such calculation.

7.10.1 For any Service Deployment/Change occurring with respect to the Service Levels provided in Sections 7.1 and 7.2: if the Service Deployment/Change exceeds the Service Level period by more than one (1) day but less than or equal to seven (7) days, one (1) Credit per day of DDoS Service delay shall apply; if the Service delay is greater than seven (7) days, thirty (30) Credits shall apply.

7.10.2 For any Service Change occurring with respect to the Service Levels provided in Section 7.4: if the Service Change exceeds the Service Level period by more than one (1) hour but less than or equal to twenty-four (24) hours, one (1) Credit per hour of Service delay shall apply; if the Service delay is more than twenty-four (24) hours, thirty (30) Credits shall apply.

7.10.3 For any Service Outage occurring with respect to the Service Levels provided in Section 7.5:

(a) if the Service Outage for Layer 3 or Layer 4 of the OSI Model is greater than five (5) minutes, but less than or equal to fifteen (15) minutes, one (1) Credit shall apply; if the Service Outage for Layer 3/4 is greater than fifteen (15) minutes, but less than or equal to sixty (60) minutes, two (2) Credits shall apply; if the Service Outage for Layer 3 or Layer 4 is greater than sixty (60) minutes, but less than or equal to four (4) hours, ten (10) Credits shall apply; and if the Service Outage for Layer 3 or Layer 4 is greater than four (4) hours, fifteen (15) Credits shall apply.

(b) if the Service Outage for Layer 7 of the OSI Model is greater than fifteen (15) minutes, but less than or equal to thirty (30) minutes, one (1) Credit shall apply; if the Service Outage for Layer 7 is greater than thirty (30) minutes, but less than or equal to sixty (60) minutes, two (2) Credits shall apply; if the Service Outage for Layer 7 is greater than sixty (60) minutes, but less than or equal to four (4) hours, ten (10) Credits shall apply; and if the Service Outage for Layer 7 is greater than four (4) hours, fifteen (15) Credits shall apply.

7.10.4 For any Service Outage occurring with respect to the Service Levels provided in Section 7.6, if more than five percent (5%) but less than fifteen percent (15%) of dirty/malicious traffic is passed to Customer Endpoint(s), five (5) Credits shall apply; if more than fifteen percent (15%) but less than twenty-five percent (25%) of dirty/malicious traffic is passed to Customer Endpoint(s), ten (10) Credits shall apply; and if more than twenty-five percent (25%) of dirty/malicious traffic is passed to Customer Endpoint(s), thirty (30) Credits shall apply.

7.10.5 For any Service Outage occurring with respect to the SLA provided in Section 7.7:

(a) if the Service Outage for Level 1 Notification is greater than five (5) minutes, but less than or equal to fifteen (15) minutes, one (1) Credit shall apply; if the Service Outage for Level 1 Notification is greater than fifteen (15) minutes, but less than or equal to sixty (60) minutes, five (5) Credits shall apply; if the Service Outage for Level 1 Notification is greater than sixty (60) minutes, but less than or equal to four (4) hours, ten (10) Credits shall apply; and if the Service Outage for Level 1 Notification is greater than four (4) hours, fifteen (15) Credits shall apply.

(b) if the Service Outage for Level 2 Notification or Level 3 Notification is greater than fifteen (15) minutes, but less than or equal to thirty (30) minutes, Customer will be credited an amount equal to twenty-four (24) times the hourly cost of the DDoS Detection and Alerting Services for the affected domain ("DDoS Service Credit"); if the Service Outage for Level 2 Notification or Level 3 Notification is greater than thirty (30) minutes, but less than or equal to sixty (60) minutes, five (5) DDoS Service Credits shall apply; if the Service Outage for Level 2 Notification/3 is greater than sixty (60) minutes, but less than or equal to four (4) hours, ten (10) DDoS Service Credits shall apply; and if the Service Outage for Level 2 Notification or Level 3 Notification is greater than four (4) hours, fifteen (15) DDoS Service Credits shall apply.

7.10.6 For any Service Outage occurring with respect to the SLA provided in Section 7.8, once provisioned, if during any one (1) day period, Cox fails to monitor Customer domain for a period of one (1) hour or more, Customer will be credited an amount equal to twenty-four (24) times the hourly cost of the Monitoring and Alerting Services for the affected domain ("Monitoring Service Credit"). Customer cannot receive more than one (1) Monitoring Service Credit per day.

7.11. Examples of Credit Calculation - Traffic Scrubbing (Section 7.10.4). For example, if Traffic Scrubbing allows more than 15% of dirty/malicious traffic to be passed to Customer but less than 25%, then the Service Credit due to Cox during that month is calculated as follows:

* $3,000 Customer Monthly Fees for that Measurement Period
* Service Credit = ($3,000 / 30 * 10) or $1,000

LIMITATIONS/USE OF CREDITS.

7.12 Limitations. Cox shall not be liable for a Service Outage if the outage is due, in whole or in part, to any of the following causes:

7.12.1 Lack of interoperability between the DDoS Service and any Customer or third party products or services. The remedies provided for in this SLA shall not be applicable in the event of Service Outage caused by any products that the DDoS Services are required to interoperate with in order for the DDOS Services to operate with Customer's systems; including any products introduced as part of a fix or modification agreed upon between the Parties.

7.12.2 Any act or omission of a third party that is unreasonable by industry standards and which has a deleterious effect on the operation of a DDOS Service to the extent such act or omission is the cause for a DDOS Service to not otherwise meet the SLA's.

7.12.3 The existence of an event constituting Force Majeure

7.12.4 Documented delays resulting from Customer's failure to respond to troubleshooting requests or other reasonable requests from Cox.

7.13 Service Credits. Credits may only be applied toward Customer's purchase of DDoS Services.

8. COX CHANGES

8.1 DDOS Services. From time to time, Cox may make upgrades or changes to the DDoS Services which impact service commitments. Cox will provide prior notice if such changes materially diminish the functionality of the DDoS Services. In the event that a change to the DDoS Services would, in Cox's commercially reasonable discretion materially diminish service commitments contained in DDOS Terms and Conditions with Customer or otherwise materially diminish the functionality of the DDoS Service ("Change"), Cox shall provide Customer with written notice at least thirty (30) days prior to the date the Change is to take effect. Any use of the DDoS Service by Customer after the Change is implemented will be deemed acceptance of the Change by Customer.

9. CUSTOMER CHANGES

9.1 Upgrades/Downgrades. Customer may upgrade or downgrade the Services. In the case of a downgrade, Customer shall provide written notice of their intent to downgrade sixty (60) days prior to the effective date of such downgrade. In the case of an upgrade, such will become effective on the first day of the month in which Cox was notified of the upgrade. In the event Customer wishes to upgrade their clean traffic package level effective one (1) month prior to the month that notice is given, and Customer makes such request within the first ten (10) days of a calendar month, Cox will discuss such request and possible alternative on a case by case basis. In addition, the following shall also apply where applicable: Configuration Change Fees, Deployment Fees. For the sake of clarity, in certain cases, Customers may not be able to downgrade between services. Additionally, any downgrade will, as applicable, take effect on the first day of the month following the sixty (60) day period.

10. SUSPENSION/TERMINATION

10.1 Suspension. Cox may suspend provision of the DDoS Services if, in Cox's reasonable determination, an Abuse occurs. Such suspension shall remain in effect until Customer corrects the applicable Abuse. In the event that, in Cox's reasonable determination, an Abuse is critically impacting, or threatens to critically impact, the Cox's network or servers, Cox may suspend provision of the DDoS Service, as applicable, immediately and without prior notice. In the event that an Abuse is not critically impacting the Cox network or threatening to do so, Cox shall give Customer prior notice of any suspension. Such suspension shall remain in effect until Customer corrects the applicable Abuse.

10.2 Termination (Abuse). If Customer fails to correct any Abuse within five (5) days after notice from Cox, Cox may, in its sole discretion, terminate its provision of DDoS Services for breach without any liability or obligation to Customer for any DDoS Service suspended or terminated.

10.3 Termination (Breach). In the event of Customer's breach of these DDoS Terms and Conditions or breach under Customer's Service Agreement, Cox may, in its sole discretion and upon written notice to Customer, immediately terminate the provision of DDoS Services, or any portion thereof.

11. WARRANTY; DISCLAIMER

11.1 Customer represents and warrants that: (a) Customer has all right, title and interest or is the licensee with right to use and/or access all of the Endpoints, applications and/or content Customer delivers to Cox to perform the DDoS Services and all of the content accessed by Cox at Customer's direction to perform the DDoS Services (collectively, "Content"); (b) Customer has the right to grant Cox the access rights and licenses set forth herein and has obtained or will obtain prior to Cox's performance of DDoS Services all rights, authorizations or permissions required for Cox to perform the DDoS Services; (c) Customer warrants that its provision of the SSL certificate for the HTTPS Packet Inspection service and Cox's use thereof for provision of the DDoS Service does not violate any laws, security policies or regulations or infringe the proprietary or privacy rights of any third party; (d) that it shall not use the DDoS Services for any unlawful purpose; (e) Customer shall comply with all applicable acceptable use policies provided by Cox in writing from time to time; and (f) Customer will not use, or allow use of, the DDoS Services in a manner that: (i) is prohibited by any law or regulation or Cox AUP, or (ii) will disrupt third parties' use or enjoyment of the DDoS Services.

11.2 Specific Warranties. In addition, Customer represents and warrants that:

11.2.1 Customer is familiar with the Foreign Corrupt Practices Act ("FCPA") and in particular the Act's prohibition on payments, or giving anything of value, either directly or indirectly, by a United States company or a company that issues United States securities, to an official of a foreign government or to other forbidden recipients for the purpose of influencing an act or decision in the official's or recipient's official capacity, or inducing such persons to influence the foreign government, to assist a company in obtaining or retaining business. Customer agrees that no part of Customer's compensation or own funds will be used for any purpose that could constitute a violation of the FCPA. Customer agrees that it does not desire and will not request any service or action by Customer that would constitute such a violation. Customer has not, and agrees that it will not hire or in any other way retain a foreign official, a foreign political party, or official thereof, or official of an international organization, or a candidate for foreign political within any sales territory.

11.2.2 Customer will comply with all applicable export and import laws, restrictions, and regulations of the United States or other applicable foreign agency or authority. The DDOS Services are for use by Customer solely for Customer's internal business purposes and not for resale to any third party, including by way of a service bureau or facilities-based service provider.

11.2.3 Customer is not a party identified on any governmental export exclusion lists and will take appropriate measures to ensure that Customers, agents and subcontractors are not in or from countries subject to U.S. embargo or identified on governmental export exclusion lists.

11.3 DISCLAIMER. THE DDoS SERVICES ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS. COX MAKES NO WARRANTY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED, TO ANY WARRANTIES EITHER INFACT OR BY OPERATION OF LAW STATUTORY OR OTHERIWISE, INCLUDING WARRANTIES OF TITLE, NON-INFRINGMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE, REGARDING THE DDoS SERVICES OR THE RESULTS TO BE OBTAINED FROM ITS USE. DDoS SERVICES PROVIDED ARE A COMMERCIALLY REASONABLE SERVICE AND COX DOES NOT WARRANT THAT THE DDoS SERVICES OR EQUIPMENT SHALL BE ERROR-FREE, UNINTERRUPTED, SECURE OR THAT MALICIOUS TRAFFIC WILL NOT REACH AN ENDPOINT OR THAT CLEAN TRAFFIC WILL REACH AN ENDPOINT. FURTHER, COX EXERCISES NO CONTROL OVER, AND ACCEPTS NO RESPONSIBILITY FOR CONTENT OR INFORMATION, INCLUDING, WITHOUT LIMITATION, CONTENT PROVIDED ON ANY THIRD-PARTY WEB SITES LINKED TO THE COX WEB SITE. COX DOES NOT ADOPT NOR WARRANT THE ACCURACY OF OR THE CONTENT OF ANY LINKED WEB SITE. THE INTERNET CONSISTS OF MULTIPLE PARTICIPATING NETWORKS THAT ARE SEPARATELY OWNED AND THEREFORE ARE NOT SUBJECT TO THE CONTROL OF COX. COX DOES NOT WARRANT THE DDoS SERVICES AGAINST MALFUNCTION OR CESSATION OF INTERNET SERVICES BY INTERNET SERVICE PROVIDERS OR OF ANY OF THE NETWORKS THAT FORM THE INTERNET WHICH MAY MAKE THE DDoS SERVICES TEMPORARILY OR PERMANENTLY UNAVAILABLE.

12. LICENSE GRANT

12.1 Customer acknowledges that operation and performance of the DDoS Services involves repeated filtering of traffic to the Endpoint and Customer hereby expressly consents to the same. Customer hereby grants Cox, for the Term, a non-exclusive, non-transferable, and royalty-free license to access the Endpoint and the internet traffic flowing thereto and any applications contained therein for the sole purpose of performing the DDoS Services.

13. GENERAL

13.1 Export Control. Customer acknowledges that Customer is subject to regulation by agencies of the U.S. Government, including regulations which prohibit export or diversion of certain data, equipment, technology, hardware and software to certain countries. Any and all obligations of Customer to provide to Customer any data, equipment, technology, hardware or software shall be subject in all respects to such United States laws and regulations as shall from time to time govern the license and delivery of equipment, technology, hardware and software abroad by persons subject to the jurisdiction of the United States.

13.2 Reservation of Rights. All rights not expressly granted to Customer herein are reserved by Cox.

13.3 Health Insurance Portability and Accountability Act (HIPAA). If Customer's traffic could contain Protected Health Information ("PHI") as defined under HIPAA, Customer agrees that: (a) Customer is responsible for appropriate security measures for the traffic, including without limitation, encryption, (b) Cox will not know if the traffic is or is not PHI, (c) the DDoS services provided by Cox are conduit services and Cox is not a business associate to Customer under HIPAA, and (d) Customer will defend, indemnify, and hold harmless Cox and its contractors for any third party Claims, including Claims made by regulatory agencies such as Health and Human Services, arising out of Customer's use of the DDoS services. For purposes of this Agreement the term "Claims" shall include without limitation, any fines, attorneys' fees, and costs incurred.