DDOS MITIGATION SERVICES ADDENDUM

1. DESCRIPTION OF DDOS MITIGATION SERVICES. Fidium will provide Distributed Denial-of-Service (**"DDoS"**) mitigation services (**"DDoS Mitigation Services"**) to you as set forth on your order for DDoS Mitigation Services under the Agreement or a separate service order for DDoS Mitigation Services (a **"Service Order"**). Each Service Order will identify the scope of the DDoS Mitigation Services and/or equipment that is the subject of such Service Order. The DDoS Mitigation Services provide attack detection, mitigation and management to help you to identify and mitigate DDoS attacks on your network, and aids you in receiving legitimate electronic traffic. During a DDoS attack, the DDoS Mitigation Services work by, among other things, diverting Internet traffic for attacked networks to a mitigating service.

2. PERFORMANCE STANDARDS OF DDOS MITIGATION SERVICES.

2.1. General. The DDoS Mitigation Services actively monitors for DDoS attacks. Should an attack be identified, Fidium will begin scrubbing attack traffic... You will be notified via electronic communication (i) when Fidium has begun to mitigate a DDoS attack and (ii) when the DDOS Mitigation Service has cleared the DDOS attack. It is your responsibility to maintain the correct email address notification list with Fidium for these notifications and any changes to email notification list must be communicated to Fidium on a timely basis. You may experience data loss, latency and other delays during the DDOS attack, and during the time that DDoS Mitigation Services are being deployed. Fidium does not guarantee complete mitigation of a DDoS attack.

2.2. Time-to-Mitigation Objective. Mitigation resolution times may vary. Fidium will notify you upon completion of mitigation scrubbing. Certain cases may require Fidium to enact a Remotely Triggered Black Hole (**"RTBH"**) to aid in clearing the DDoS attack, which would result in a total loss of your data service as the RTBH is enacted. Fidium will inform you prior to enacting this RTBH methodology.

2.3. Repair and Scheduled Maintenance. Repair efforts will be undertaken upon notification of trouble by internal network surveillance and performance systems or by notification of trouble and release of DDoS mitigation service by you for testing. You will be notified a minimum of five (5) business days in advance of any scheduled maintenance. Scheduled maintenance will be performed in a manner that minimizes any system interruption. Performance and availability standards will not apply during scheduled maintenance periods.

3. LIMITATIONS. Fidium's performance of the DDoS Mitigation Services is dependent on you: (i) undertaking all customer responsibilities contained in the Agreement and (ii) timely cooperating with Fidium with respect to any other customer requirements specified by Fidium for operation of DDoS Mitigation Services. DDoS Mitigation Services are intended to improve your ability to mitigate a DDoS attack, but your use of DDoS Mitigation Services does not guarantee: (i) the security of your data, information or network; or (ii) that any DDoS attack will be completely mitigated. Fidium DISCLAIMS ANY AND ALL REPRESENTATIONS OF WARRANTIES, EXPRESS OR IMPLIED, IN FACT OR BY LAW, STATUTORY OR OTHERWISE, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR USE, AND THAT DDOS MITIGATION SERVICES WILL BE UNINTERRUPTED OR ERROR FREE, OR THAT YOUR NETWORK SERVICES WILL BE UNINTERRUPTED OR ERROR FREE WITH USE OF DDOS MITIGATION SERVICES. Fidium will provision DDoS Mitigation Services according to the standards set forth in the applicable Agreement. In the event of any breach of your data or information, due to any cause, Fidium's liability (and limitations thereof) for such breach, and any failure of DDoS Mitigation Services, is as forth in the applicable Agreement.