

DIABLO DATA, LLC

ROBOCALL MITIGATION PLAN

Diablo Data, LLC ("Diablo Data") provides wholesale VoIP solutions for retail service providers using a white-label IP-based voice services provider, Momentum Telecom, Inc ("Momentum"). Diablo Data also provides broadband monitoring, provisioning, and managed support services. In addition to our upstream service provider having implementing STIR/SHAKEN on its network, Diablo Data has adopted this robocall mitigation plan to take its own measures to limit the potential for the originating, carrying, or processing of unlawful robocalls from or on its network.

Know-Your Customer Policies:

Wholesale Services:

Diablo Data vets the identity of its wholesale customers prior to entering a contract for VoIP services. As part of this vetting process, Diablo Data collects the wholesale customer's business name and address, physical location, contact information, jurisdiction of incorporation, federal tax ID, FCC Form 499 identification number and federal Universal Service Fund contributor status, and the nature of the wholesale customer's business. This information may be provided to third party agencies to determine the credit and/or fraud risk associated with the wholesale customer. If Diablo Data cannot validate the customer based on the initial information provided, Diablo Data may require additional information to validate the customer to seek to ensure it is operating a legitimate business as a reseller of Diablo Data's VoIP services. Diablo Data will not provide service if a new wholesale customer's identification cannot be verified.

Diablo Data's wholesale customers are expected to vet their end user subscribers consistent with the FCC's robocall mitigation rules. Diablo Data will in good faith collaborate with its customers to exchange relevant information regarding efforts to reduce unlawful robocalls and respond to request from the Industry Traceback Group (ITG), as described below. Diablo Data's contracts require cooperation with Diablo Data in responding to ITG traceback requests and prohibit the use of its services to originate unlawful traffic, as reflected in the following contract provisions:

(A) Cooperation with Traceback Requests. Customer agrees that when it is acting as an upstream provider originating traffic (hereinafter referred to as an "Originating Provider") or an upstream provider passing traffic through (hereinafter referred to as a "Transit Provider"), if it receives a request from (i) a traceback administrator authorized by the USTelecom Industry Traceback Group (ITG), (ii) Diablo Data, or (iii) any applicable law enforcement or regulatory authority (hereinafter referred to as a "Traceback Requestor") for information about robocalls that have been sent to a downstream provider or received by a consumer (hereinafter referred to as a "Traceback Request"), Customer will respond to the Traceback Request in good faith within twenty-four (24) hours. Customer agrees that its response shall indicate if it is in the call path as the Originating Provider of the calls (i.e., Customer received the calls from Customer's End User) or (ii) a Transit Provider (i.e., Customer received the calls from another voice provider). Customer shall also identify the source of the calls to Customer's network and provide other relevant information relevant to the determination of the source, and, to the extent possible, shall

further identify any other upstream providers in the call's path. Customer agrees to share this information without requiring a subpoena or other formal demand or request. Customer is not required to respond to more than ten (10) Traceback Requests per week from Traceback Requestor(s). In the event Customer fails to promptly respond to Traceback Requests (in no event to exceed twenty-four (24) hours), Diablo Data may, upon not less than fifteen (15) days' prior written notice to Customer with an opportunity to cure, terminate any services that Diablo Data is providing to Customer that involve the termination of Customer's IP calls, including without limitation, SIP Gateway Service, SIP Gateway Outbound Service, and Global IP Connect Service (collectively, referred to as "IP Termination Services").

(B) Customer's Upstream Providers. Customer shall require all upstream providers from whom it receives traffic to comply with the requirements of this Amendment. Customer is not required, however, to require its upstream providers to provide information directly to Diablo Data in response to any Traceback Request. In the event any provider in the call path refuses to respond to a Traceback Request, Customer agrees that a Traceback Requestor may provide all providers in the call path with information sufficient to ascertain the identities of all the providers in the call path to allow each provider to enforce the traceback participation requirement directly against its upstream provider.

(C) Illegal Use of IP Termination Services. Notwithstanding anything to the contrary contained in the Services Agreement, if Diablo Data determines Customer's IP Termination Services are being used to support illegal robocalling activity, or Customer fails to cooperate with Diablo Data, to Diablo Data's reasonable satisfaction, in addressing robocalling activity attributable to Customer's IP Termination Services with a goal of eliminating illegal robocalls, Diablo Data may, upon not less than thirty (30) days' prior written notice to Customer, terminate any IP Termination Services.

To the extent a wholesale customer is found to have violated its contractual obligations for the reasons noted previously or any other reason, Diablo Data will act commensurate with the severity of the customer's offense, including, but not limited to, providing the customer with a warning or terminating the customer's service.

Use of Call Analytics to Identify and Block Unlawful Traffic

Diablo Data's upstream provider (Momentum) has implemented its own call analytics to identify unlawful traffic originated by the end users of Diablo Data's wholesale customers' services, and provides Diablo Data with access to this information. Call analytics detect call patterns that indicate robocall activity, including, but not necessarily limited to, an unusually substantial number of calls from the same number, an excessive number of short duration calls, and calls that stop attempting to connect after a single ring. Call analytics also can detect where the calling number is invalid, unallocated, or on ITG's Do Not Originate ("DNO") list. If call analytics detect any of the above-described issues, an internal report is generated that summarizes the issues presented and the applicable wholesale or retail customer that is responsible for the underlying calls.

If our analytics report indicates potential illegal robocall activity by a wholesale end user customer, Diablo Data alerts the wholesale customer's contact representative and asks the customer to investigate the issue and thereafter inform Diablo Data: (i) when the issue is resolved and (ii) what actions the wholesale customer took in resolving the issue.

If our analytics report indicates potential illegal robocall activity by one of its own retail customers, Diablo Data conducts its own investigation into the customer and the calls at issue. After concluding its investigation, Diablo Data will act commensurate with the severity of the customer's offense, including, but not limited to, providing the customer with a warning or terminating the customer's service and/or reporting the misconduct to the appropriate authorities.

Knowledge of Upstream Providers

Diablo Data knows all the upstream providers from which it directly receives traffic and has insight into its upstream providers' policies and procedures related to identifying and blocking unlawful robocall traffic through Diablo Data's review of these providers' robocall mitigation plans. Diablo Data confirms that all upstream providers from which it receives traffic are listed in the FCC's Robocall Mitigation Database.

Cooperation with the Traceback Group, Law Enforcement and Government Agencies

Diablo Data is committed to responding fully and within 24 hours to all traceback requests made by ITG, law enforcement authorities, and government agencies to investigate and address suspected unlawful robocalls originated or passed to Diablo Data. Diablo Data's wholesale contracts require its wholesale customers to cooperate with Diablo Data in responding to ITG traceback requests, as detailed above.

Diablo Data is committed to fully complying with the Commission's robocall blocking requirements and confirms that it will block all calls and provider traffic that: (1) are identified in any public notice or order released by the FCC; (2) are substantially similar to the types of traffic identified in any public notice or order released by the Commission; or (3) include a caller ID number or name that is on DNO list issued by ITG. Diablo Data's upstream provider also blocks the traffic of all foreign providers and gateway providers that have not registered in the Robocall Mitigation Database.

Principal: James A. Clark, Sole Member of LLC

E-mail: jim.clark@diablodata.com

Phone: 1-678-636-9741