

Phaeton Services Corporation Gateway Provider Robocall Mitigation Plan

Phaeton Services Gateway Provider Robocall Mitigation Plan Phaeton Services Gateway. a New York Corporation (Phaeton), hereby submits this Robocall Mitigation Plan ("Plan") as required by 47 CFR Sec. 64.6305(b) & (d) and the Federal Communications Commission ("Commission"). The Plan describes the actions Phaeton takes with respect to foreign-originated robocalls carrying US numbers in the caller ID field. Phaeton provides international voice services for wholesale carriers in both the US and internationally. Phaeton does not originate or terminate any voice calls bound for the US, instead it serves as an Intermediate Provider for other wholesale carriers. As explained in more detail below, Phaeton has implemented various policies and practices consistent with the Commission's requirements for Gateway Providers. These practices are designed to prevent, as much as reasonably possible, the transit of illegal robocalls destined for the US. The following describes the reasonable steps that Phaeton has implemented to mitigate foreign originated robocall traffic carrying a U.S. number in the Caller ID field.

Call Authentication/Signing Phaeton has implemented technical procedures to pass unaltered any identity header it receives with calls using Session Initiation Protocol (SIP) on the IP portions of its network to terminating voice service providers or subsequent intermediate providers in the call path. As required by the FCC's STIR/SHAKEN Order, LOOK has implemented the required Gateway provider implementation of STIR/SHAKEN authentication for calls into the US with NANPA US numbers in Caller ID Field.

Traceback Cooperation and 24 Hour Response Phaeton commits to responding fully and within 24 hours to traceback requests from the industry traceback consortium, civil and criminal law enforcement and the Commission, and to cooperate in investigating and stopping any identified illegal robocallers that use Phaeton US Gateways to carry or process calls. To the extent feasible within 24 hours, Phaeton will provide the identity of the upstream provider with which it is directly connected, the country, address, contact information for that provider, and a link to that provider's robocall mitigation database filing if applicable. Phaeton, in turn, requires its upstream customers to provide information to Phaeton within the same allotted period so that Phaeton may properly and promptly investigate a traceback request. Phaeton will impose restrictions, including suspension or termination, for upstream carriers who generate multiple traceback requests.

Mandatory Blocking Following Commission Notification Upon receipt of a notice from the Commission's Enforcement Bureau that it is a Gateway Provider for suspected illegal traffic, Phaeton will immediately investigate the identified traffic and begin blocking the traffic, including traffic determined to be substantially similar to the identified traffic, within the time

specified in the notice. Phaeton will make a good faith effort to identify substantially similar traffic considering common indicia of illegal calls such as call duration, call completion ratios, large bursts of calls in a short time frame, neighbor spoofing patterns and sequential dialing patterns. Where Phaeton does business with the identified entity or associated parties, Phaeton will block all US inbound traffic immediately and permanently.

Customer Due Diligence –

Phaeton conducts a comprehensive due diligence and credit review before establishing a contractual relationship with carrier customers. This includes a thorough research on the prospective carrier's industry reputation and the required completion of "Know Your Customer" form.

Phaeton contracts establish a reciprocal general obligation between Phaeton and its carrier customers to not use the services for any unlawful purpose, to prevent fraudulent uses, and to cooperate with each other to avoid these unlawful activities.

Phaeton will terminate or suspend service to customers with a history of non-compliance with its contractual obligations, including provisions relating to acceptable use of the service.

Other Internal Policies

Phaeton will block traffic that appears to be illegal or is flagged as suspicious under its fraud policy.

Phaeton will make a good faith effort to identify substantially similar traffic considering common indicia of illegal calls such as call duration, call completion ratios, large bursts of calls in a short time frame, neighbor spoofing patterns and sequential dialing patterns.

Phaeton implements network wide blocking of incoming traffic based upon the "Do Not Originate" list. - Phaeton also implements several manual resource efforts to evaluate the legitimacy of incoming voice communications. Phaeton will periodically evaluate the risks it faces, the effectiveness of its policies and procedures, and its capabilities to support the measures described. Should it determine that changes are appropriate, its practices may differ from those described on this document.

Phaeton participates in Telco-Industry-Wide Fraud Mitigation Activities and is committed to comply with the following principles:

1. Targets for prevention of fraudulent traffic to be included within management reporting.
2. Carriers to adhere to i3 Forum recommended processes to detect and avoid fraud.
3. Identified fraudulent number ranges and destinations to be blocked.

4. All reasonable action will be taken to avoid payment flows to the instigators of fraudulent traffic.

5. Commitment to share information regarding fraudulent traffic flows with other carrier peers.

6. Adoption of standard contracting terms addressing fraudulent traffic management.

Phaeton will periodically evaluate the risks it faces, the effectiveness of its policies and procedures, and its capabilities to support the measures described.