

Frontier IOT Robocall Mitigation Plan

Frontier IOT is committed to complying with the Federal Communications Commission (FCC) regulations under 47 C.F.R. § 64.6305 to mitigate and eliminate the origination of illegal robocalls on its network. This document outlines Frontier IOT's current policies and procedures designed to reduce or eliminate outbound illegal robocalls originating on its network. Frontier IOT Company undertakes to take "reasonable measures" and responding to all traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG), and to cooperate with such entities in investigating and stopping any illegal robocallers that may use its service to originate calls.

1. CUSTOMER CONTRACT AND COMPLIANCE REQUIREMENTS

All Frontier IOT customer agreements explicitly prohibit passing illegal robocalls through any of our switches or networks and define precise requirements for ASR, LCD and other traffic statistics and violations will result in immediate service termination. Frontier IOT requires all customers to provide true and valid information about business such as physical location, contact personnel, state/country of incorporation or business formation, federal tax I.D. or non-USA government I.D. They must also disclose the practices and nature of their business. We endeavor to know the precise type of traffic which originates from each customer's switch including the type of customers they acquire and exact type of services they provide. Frontier IOT vetting process is intended to help determine the legitimacy of a customer for the purpose of establishing a service relationship.

2. MONITORING AND TRACEBACK

Frontier IOT monitors its system diligently and will investigate any suspicious traffic. When we detect suspicious traffic, we will immediately take appropriate actions to ensure that it is legitimate. In the event Frontier IOT receives a traceback request for an illegal robocall, we act on it immediately, request a specific and detailed explanation from our customer(s) and insist on immediate corrective action. If the customer fails to take timely corrective action, Frontier IOT will immediately terminate services and escalate the matter to law enforcement authorities. To allow for timely and comprehensive law enforcement response efforts against illegal robocallers, Frontier IOT will dedicate sufficient resources to promptly complete and provide responses to all traceback requests received from the FCC, law enforcement and/or the ITG, and commits to fully responding to any traceback.

3. INTERNATIONAL CALL ORIGINATORS

Frontier IOT is not currently an international voice services provider. If at any time the Frontier IOT does sell its services to customers which are international call originators using North American Numbering Plan resources it will familiarize itself with and develop best practices for fulling vetting such customers and performing telephone number validation on all international originated calls.

4. CALL BLOCKING AND VALIDATION

Frontier IOT blocks all calls originating from numbers known to us to send illegal robocall traffic and/or calls destined to specific phone numbers as appropriate for robocall mitigation. Frontier IOT enforces telephone number validation procedures, for: (1) single line voice service subscribers, both services connected via TDM or IP, the switching equipment has been set up to only accept calls from the number assigned to that subscriber; and (2) subscribers with multi-line telephone systems, for both services connected via TDM or IP, the Provider screens all originating calls and only allows calls to be connected if the originating number matches one of the numbers assigned to the subscriber. These screening capabilities enable an automated and secure method of validating originating telephone numbers.

5. LAW ENFORCEMENT COOPERATION

Frontier IOT cooperates fully with investigative authorities, industry traceback groups, the FCC and the official consortium designated to lead private traceback efforts. We have a single contact individual designated to handle all traceback requests and coordinate with outside investigations.

6. CONTINUOUS IMPROVEMENT MEASURES

To ensure ongoing alignment with regulatory requirements and industry advancements, Frontier IOT implements the following continuous improvement measures: (1)Frontier IOT conducts regular reviews of call detail records (CDRs) to detect anomalies. (2)Frontier IOT proactively updates its call-blocking databases and third-party tools while conducting annual audits to refine mitigation strategies, ensuring alignment with evolving FCC regulations and industry best practices. (3)Frontier IOT conducts annual evaluations of the Robocall Mitigation Plan's effectiveness, refining strategies as needed to address emerging fraud tactics and ensure compliance with evolving FCC regulations and industry standards.