

iBASIS Inc.

Gateway Provider Robocall Mitigation Plan

iBASIS Inc. a Delaware Corporation (“iBASIS”), hereby submits this Robocall Mitigation Plan (“Plan”) as required by 47 CFR Sec. 64.6305(b) & (d) and the Federal Communications Commission (“Commission”) Public Notice dated December 12, 2022, *In The Matter of Call Authentication Trust Anchor*, WC Docket No. 17-97, DA 22-1303 (“Robocall Notice”). The Plan describes the actions iBASIS takes with respect to foreign-originated robocalls carrying U.S. numbers in the caller ID field.

iBASIS provides interstate and international voice and data telecommunications and associated value-added services for wholesale carriers in both the US and internationally. iBASIS does not originate or terminate any voice calls and has no voice end users, instead it serves as an intermediate voice carrier for other wholesale carriers. At times, for certain foreign originated calls destined for the U.S., iBASIS is a Gateway Provider as described by the Commission and it files this Plan in that capacity.

As explained in more detail below, iBASIS 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 U.S.

The following describes the reasonable steps that iBASIS has implemented to mitigate foreign-originated robocall traffic carrying a U.S. number in the caller ID field.

1. Traceback Cooperation and 24 Hour Response

iBASIS commits to responding fully and within 24 hours to Traceback Requests from the Industry Traceback Group (“ITG”), civil and criminal law enforcement and the Commission, and to cooperate in investigating and stopping any identified illegal robocallers that use iBASIS US Gateways to carry or process calls.

2. Mandatory Blocking Following Commission Notification

Upon receipt of a notice from the Commission’s Enforcement Bureau that iBASIS is a Gateway Provider for suspected illegal traffic, iBASIS will immediately investigate the identified traffic and block the traffic from the provider within the time specified in the notice. iBASIS will make a good faith effort to identify and block 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.

3. Blocking DNO Calls

iBASIS implements network wide blocking of incoming traffic based upon the USTelecom “Do Not Originate” list, and have augmented this further with the SOMOS DNO list. iBASIS also has implemented a DNO list provided by the Social Security Administration in Q4 of 2020.

4. Know Your Upstream Provider (“KYC”)

iBASIS applies a comprehensive due diligence process to assess and manage the risk associated with upstream providers up front. This process is designed to evaluate the potential traffic profile and legal compliance of these providers prior to onboarding. iBASIS’ KYC procedures include the following key components:

- The Sales and Product Management teams conduct risk assessments of potential upstream providers. This includes evaluating: the type of traffic the customer intends to send, the types of end users served by the provider, and the primary destinations to which traffic will be routed. As part of this process, prospective upstream providers are required to complete a comprehensive “know your customer” form that captures information such as: the nature of the provider’s business and traffic, whether provider engages in robocalling and the service types associate with such traffic, the use of U.S. NANP to U.S. NANP number ranges, engagement and cooperation with the ITG, the provider’s status and compliance in the robocall mitigation database (“RMD”), and provider’s familiarity with US laws regarding illegal or nuisance calls to U.S. consumers. Completed forms are reviewed by the Voice Product Management team to determine risk levels and to decide whether to authorize the provider’s traffic for termination within the U.S.
- All prospective upstream providers must submit verifiable business information: legal business name, business address, contact details and tax or other regulatory ID. The Finance Department reviews this information to evaluate provider’s legitimacy, and when applicable, credit worthiness and risk level. iBASIS utilizes search engines and third-party tools to confirm the legitimacy and risk exposure of the business entity.
- The Legal Department screens potential customers and their authorized signatories are screened against international economic sanction lists, including but not limited to the U.S. Office of Foreign Assets Control (OFAC).
- iBASIS' customer agreements for new upstream voice providers include specific clauses requiring the provider to warrant that it has implemented a “Stir/Shaken” call authentication framework and/or other robocall mitigation practices, including but not limited to a robocall mitigation plan, in which it (1) takes reasonable steps to avoid originating illegal robocall traffic and (2) commits to cooperate in investigating and stopping any robocalls, i.e., blocks calls believed to be illegal, including cooperation with applicable industry trade groups such as the ITG. For existing customers who have been blocked due to a Traceback Request and who seek to resume sending U.S. NANP to U.S. NANP traffic, iBASIS requires them to sign a contractual amendment committing to (i) cooperate with the ITG overseen by USTelecom; (ii) respond within 24 (twenty-four) hours to requests for Traceback Information (“Traceback Request”) received from iBASIS and the ITG administrator; (iii) take immediate action to

block the number in question that is the subject of a Traceback Request; (iv) materially conform to ITG policies and procedures as they may be amended from time to time and as set forth in set forth in the USTA website (<https://www.ustelecom.org>).

5. General Mitigation Efforts: Analytics & Call Handling

iBASIS utilizes a combination of automatic systems and manual resource efforts to evaluate the legitimacy of incoming voice traffic and identify potentially illegal communications, including unlawful robocalls. iBASIS has implemented and adheres to a defined process for detecting suspicious or high-risk traffic, including robocalls. Processes include:

Automated Detection with Manual Verification and Action

iBASIS has implemented automated analytics with specific parameters applied across all incoming traffic on a network-wide basis to detect suspicious patterns often associated with fraudulent traffic. Daily reports highlighting suspicious traffic flows are reviewed same day by the Operations Department. The review includes:

- **Review** - Verification consists of some or all of the following elements as necessary:
 - Comparison of historical traffic patterns to the suspect traffic patterns from the customer in question
 - Comparison of traffic patterns to other customer traffic
 - Manual test calls placed to the calling number
 - Evaluation of quality statistics on the traffic in question to determine if providers are rejecting an abnormal proportion of the traffic or if completion rates are substantially lower than normal.
- **Call Handling** - Actions taken are based on pre-defined thresholds:
 - If the volume of traffic in a daily report meet a certain threshold indicating a high likelihood of suspicious traffic, iBASIS will manually block the customer's traffic that day. The assigned account manager is notified to begin an investigation with the customer to determine the legitimacy of the traffic.
 - If traffic patterns do not meet the blocking threshold, but the traffic pattern raises a concern, iBASIS will not immediately block the traffic. Instead, the account manager will engage the customer to proactively verify the legitimacy of the traffic.
- **Documenting and Tracking** - All communications and resolutions related to suspicious and potentially illegal traffic, including robocalls originating from US +1 to US +1, are documented in iBASIS' internal trouble ticket system.

Automated Detection with Automated Verification and Action

iBASIS' proprietary FraudLock system, adopted in 2012 and periodically enhanced, contains business rules and intelligent algorithms to monitor certain carriers' traffic crossing the network on a 24/7 basis.

- **Review** - FraudLock automatically detects "suspicious" traffic patterns from carriers that

usually send non-dialer and legitimate traffic. Suspicious traffic patterns can include:

- o An unusual appearance of short duration traffic
 - o An abnormal number of calls placed to a wide array of called numbers from a single calling number
 - o Sequential strings of calling numbers placing short duration calls
 - o High instances of invalid calling numbers.
- **Call Handling** – FraudLock engages in both reactive and proactive measures to prevent ongoing or future instances of fraud, inclusive of suspicious robocalling:
 - o FraudLock system notifies the upstream provider of the suspicious traffic and executes automated blocking on the traffic matching fraudulent patterns within minutes.
 - o FraudLock automatically generates “black lists” (calling or called numbers that have been reported as fraudulent) for future automated blocking.
- **Documenting and Tracking**
 - o All instances of potential fraud and subsequent actions taken by the system are captured and stored in a secure data warehouse.
 - o Blocking actions are documented via iBASIS’ internal trouble ticket system.
 - o Historical reporting is available in iBASIS reporting system.

6. Call Authentication/Signing

As required by the FCC's STIR/SHAKEN Order, iBASIS has implemented the required Gateway provider implementation of STIR/SHAKEN authentication for calls into the US with NANPA US numbers in caller ID field. This signing includes call Reputation Scoring, reducing the risk of signing illegal robocalls and transporting through the iBASIS network.

7. iBASIS Discretionary Measures

Participation in Telco-Industry-Wide Fraud-Mitigation Activities

iBASIS remains an active member of ITW Global Leaders’ Forum (“GLF”), and has agreed to its Code of Conduct for International Carriers to take leadership in the prevention of fraud traffic. Based on the Code of Conduct, iBASIS must obey and comply with these six principles:

1. Targets for prevention of fraudulent traffic to be included in 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.