

Blue Dragon Network Robocall Mitigation Plan

This submission is intended to outline and show the commitment of Blue Dragon Network Telecom, LLC (“BDN”) to taking reasonable steps to avoid carrying illegal robocall traffic. BDN is committed to adhering to the deadlines and requirements set forth by the Federal Communications Commission (FCC) in the TRACED Act, as well as subsequent Reports and Orders. BDN continues to work with industry leaders, other service providers, and third-party solution providers to be proactive in combating against illegal robocalls.

Entity of Record:

*Blue Dragon Network Telecom, LLC
3672 Moca Dr
Saint Cloud, FL 34772
OCN: 073L*

Call Roles – Non-Gateway Intermediate Provider

- As a newly established provider, Blue Dragon Network is currently in the process of fully implementing the STIR/SHAKEN authentication framework on its entire network and expects to complete the implementation within 60 days of the submission of this filing.*
- BDN meets its existing obligations to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls by taking the following actions:*
 - Thorough KYC evaluations of all incoming clients*
 - Validate if customer has an active 499 Registration*
 - Validate that carrier is in the RMD and that the data matches.*
 - Validate carrier shows they are Stir/Shaken compliant.*
 - Validate FRN data provided.*
 - Review of customer IPs to validate true origin of operation*
 - Specific onboarding and background check requirements for each type of customer business*
 - Domestic Enterprise*
 - Fully Functional website*
 - Operational Business Number listed on website*
 - Address ownership is easily verified via Google or MelissaData and correlates with website listing*
 - If address can't be easily verified, customer must provide proof of address*
 - Ownership of Email domain (cannot be an anonymous domain like gmail / hotmail)*
 - Domestic Call Center / Contact Center*
 - Verified Address*
 - Customer honors DNC List and that marketing calls are only placed to users that have provided explicit permission to be contacted*

- Blue Dragon Network has deployed call analytics systems that identify and block illegal traffic using the following metrics on an individual number, customer, and network-wide level:

- ASR*
- ACD/ALOC*
- DNO Usage*
- DNCL Usage*
- Invalid ANI %*
- SIP 600 Level errors*
- SIP 404%*

COMMITMENTS and CERTIFICATIONS

-BDN is committed to utilizing the described steps above to mitigate illegal robocall traffic.

-BDN certifies that any calls that originate on its network are subject to the robocall mitigation program.

-Blue Dragon Network commits to respond fully within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

- Blue Dragon Network certifies that it has not been prohibited from filing in the Robocall Mitigation Database

- Blue Dragon Network has not been subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing and provide information concerning any such actions or investigations

- At no time in the prior two years, has Blue Dragon Network (or any entity for which the filing entity shares common ownership, management, directors, or control) been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing.

-BDN confirms that provisions exist in customer Terms and Conditions that allow for termination of services if any fraudulent or illegal traffic is identified.

-BDN confirms that along with internal blacklist that it is also using commercial DNO lists to block unauthorized traffic.

Traceback Request Response:

BDN actively works with the Industry Traceback Group (ITG) in the investigation of traceback requests.

Due to CPNI, BDN follows strict process of only sharing information through the official ITG portal. Upon notice via any method – phone, email, or direct engagement through the portal – an investigation is initiated promptly.

Post notification Process to mitigate illegal traffic:

- *Once we receive a Traceback, the ANI(s) involved are immediately blocked from our termination network.*
- *The result of the investigation and identification of the source is communicated to ITG via their Portal.*
- *We then report the issue to the client and ask them to take corrective action and share the steps taken.*
- *Clients not responding within 24 hours are given additional notice that their termination account will be suspended in the absence of a timely resolution.*
- *Weekly and Monthly review of Tracebacks is performed looking for any identifiable pattern.*
- *Clients triggering three or more Tracebacks in a thirty-day period and flagged for executive review.*

At a minimum, this leads to a discussion with the client regarding their traffic, and further review of their KYC process. Depending on the results of this discussion BDN may choose to close the account.

*Kitaya Stone*_____

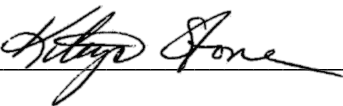
Name

*CEO*_____

Title

*9/24/2024*_____

Dated

x _____

Blue Dragon Network Robocall Mitigation Plan 09/24

*Updated: 5/16/2025*_____