



DialToneServices, L.P.

ROBOCALL MITIGATION PLAN

July 7th, 2025

ABOUT

DialToneServices is a small VSP providing Satellite Communications utilizing Iridium Communications Inc.'s (Iridium) network for all inbound and outbound call routing.

As such, DTS relies on procedures, policies, and safeguards implemented by Iridium to ensure that DTS' residential and business customers are sufficiently protected against illegal robocall and spoofing activities. Iridium has submitted an extensive Robocall Mitigation Plan to the Robocall Mitigation Database that we implement and follow, together with DTS' own mitigation efforts as detailed below.¹

TRACEBACK

DTS is committed to responding within 24 hours to all traceback requests from the Commission, law enforcement, and the registered traceback consortium and cooperates with such entities in investigating and stopping any illegal robocallers from utilizing our services.

STIR/SHAKEN

DTS is dedicated to halting illegal calls from originating in our network and monitoring incoming calls by the following Robocall Mitigation Plan. Because DTS lacks control over the network infrastructure necessary for STIR/SHAKEN implementation, it is not required to be STIR/SHAKEN compliant.²

ROBOCALL MITIGATION PLAN

¹ See Iridium Communications Inc., Robocall Mitigation Plan (filed Feb. 26, 2024), https://fccprod.servicenowservices.com/rmd?id=rmd_form&table=x_g_fmc_rmd_robocall_mitigation_database&sys_id=181b87bd1b45f4107ccf20ecac4bcb28&view=sp (Iridium RMP).

² See Call Authentication Trust Anchor, Implementation of TRACED Act Section 6(a) Knowledge of Customers by Entities with Access to Numbering Resources, WC Docket Nos. 17-97 and 20-67, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3241, 3260, para. 40 (2020).

All voice traffic that originates on our network is subject to this robocall mitigation program.

First, we would like to mention that due to the unique technical and usage characteristics of satellite voice communications, it would be difficult, if not impossible for illegal robocalls to originate from our service. DTS handsets do not support high-volume dialer traffic or caller-ID spoofing and it would be uneconomic for robocallers to use DTS' service due to the high airtime cost of satellite service.

Second, DTS reviews the Daily Call Data Records (CDRs) received from our satellite network provider, Iridium. These CDRs are analyzed and utilized for investigation of suspicious call activity. In the event that inconsistencies appear, DTS will contact customers to remedy potential robocall or fraudulent call origination. DTS will immediately investigate any suspicious calls to determine if the caller was attempting to originate unlawful robocalls. If it is determined that the caller was attempting to originate unlawful robocalls, DTS will warn the customer to stop and subsequently suspend or terminate their service. We also analyze high-volume voice network traffic, if any, to identify and monitor patterns consistent with robocalls. This information assists in the traceback process to identify the source of illegal calls.

Although we do not currently employ third-party robocall analytics vendors, the use of the Iridium satellite network-which is a secure and closed system-significantly reduces our exposure to traditional robocall vectors. Should our services expand into PSTN or terrestrial VoIP integrations, we will evaluate and implement appropriate analytics-based mitigation tools.

Lastly, DTS has a customer contract that all new and existing subscribers must sign to receive our services. Upon contract signing we require them to provide proper identification which includes but are not limited to: name, physical address, contact phone number, email, credit card information and state of formation for business subscribers further explained in the Know Your Customer section below. We have also implemented an Acceptable Use Policy for new and existing subscribers which prohibits:

- Falsifying or misrepresenting sender identity or message origin;
- Breaching any applicable local, state, or federal laws;
- Breaching applicable industry accepted guidelines; and
- Participating in or facilitating fraudulent activities using DTS service.

Subscribers are bound by contractual terms stipulating that DTS reserves the right to take disciplinary action, including suspension or termination of service, in case of AUP violations.

Alongside DTS' preventative robocall measures, Iridium has robust contractual terms and policies in place to mitigate origination of illegal robocalls such as: obligations to suspend

or deactivate voice services under certain circumstances, contractual prohibitions against least cost routing and contractual obligations to comply with all federal and state laws.³

KNOW YOUR CUSTOMER (KYC) PRACTICES

As part of our Robocall Mitigation Plan, DTS has implemented a comprehensive Know Your Customer (KYC) protocol to help prevent the origination of illegal robocalls on our network. Our KYC practices apply to all new and existing customers, both individual and business entities, and include the following verification steps:

1. Government-Issued Identification

We require a valid, government-issued photo ID (e.g., driver's license or passport) from all individual customers at the time of account setup. This ensures the identity of the individual initiating service is clearly verified.

2. Proof of Address

To confirm the residential or business location, customers must provide a recent utility bill, lease agreement, or other official document that matches the address on file. This documentation must be dated within the past 60 days

3. Location Verification

We independently verify customer-provided addresses and business locations through mapping programs and 911 verification to ensure consistency and legitimacy of the claimed address.

4. Backup Documentation

If the initial proof of address is insufficient or inconclusive, we request additional documentation such as bank statements, insurance documents, or mail from government agencies to further validate the customer's address and identity.

5. Business Customer Requirements

For business accounts, we require submission of valid business documentation, including but not limited to:

- Articles of Incorporation or Organization
- Employer Identification Number (EIN) verification
- State business license or certificate of good standing
- Contact information for the authorized representative

These measures support our commitment to preventing bad actors from exploiting our services for unlawful robocalling activity. Customer information is securely stored and reviewed periodically to ensure continued compliance.

³ See Iridium Communications Inc., Robocall Mitigation Plan: Pg. 5D (filed Feb. 26, 2024), https://fccprod.servicenowservices.com/rmd?id=rmd_form&table=x_g_fmc_rmd_robocall_mitigation_database&sys_id=181b87bd1b45f4107ccf20ecac4bcb28&view=sp (Iridium RMP).

KNOW YOUR UPSTREAM PROVIDER

DTS is a Tier 1 provider for Iridium services. As Iridium is DTS' only upstream provider, DTS has a close relationship with Iridium's Regulatory department and follows its policies to comply with the FCC's "Know Your Upstream Provider" obligations. With respect to Iridium's compliance, it operates with two to three Tier 1 upstream providers maximum at a given time to facilitate all voice traffic originating from or terminating to the Iridium network, including all calls that reach DTS customers. The relationships between Iridium and its upstream providers, as well as between DTS and Iridium as its upstream provider, are governed by strong contractual terms.⁴

FINAL

Robocall Mitigation Plans need to adapt continually to effectively combat illegal robocalling, reflecting its ever-changing nature. DTS commits to monitoring industry standards and enhancing internal procedures to ensure flexibility and responsiveness to these evolving challenges. Should any significant modifications occur, DTS will promptly communicate these changes to employees, consultants, and contractors. Additionally, DTS will revise its Robocall Mitigation Plan as necessary and file the revised plan in the Robocall Mitigation Database within ten days of any changes.

CONTACT INFO

DialToneServices, L.P.
Emily Neumaier
Chief Administrative Officer
emily@rangeglobal.com

⁴ See Iridium Communications Inc., Robocall Mitigation Plan, Page 6D (filed Feb. 26, 2024), https://fccprod.servicenowservices.com/rmd?id=rmd_form&table=x_g_fmc_rmd_robocall_mitigation_database&sys_id=181b87bd1b45f4107ccf20ecac4bcb28&view=sp (Iridium RMP).