

Gateway Robocall Mitigation Plan

Business Information

Data@ccess Communication, Inc.
316 De La Constitucion Avenue
Suite 100
San Juan PR 901

Contact for Robocall Mitigation Issues

Pablo Martinez
VP of Operations
787-977-8025
pablo.martinez@dataccesspr.com

Overview

Pursuant to FCC Rule 64.6305(b),¹ the FCC requires that, by January 11, 2023, gateway providers certify in the Robocall Mitigation Database that they have implemented a Robocall Mitigation Plan ("RMP") containing reasonable steps to avoid carrying or processing illegal robocall traffic.

The FCC requires that gateway providers develop a RMP that:

- certifies to the status of STIR/SHAKEN implementation and robocall mitigation on their networks;
- provides contact information for a person responsible for addressing robocall mitigation-related issues;
- describe in detail their robocall mitigation practices; and
- certifies that they will comply with traceback requests within 24 hours; and
- complies with their "know-your-upstream-provider" obligation.²

Purpose

Data@ccess Communication, Inc. ("Data@ccess") is a small voice service provider ("VSP") and gateway provider that is dedicated to stopping illegal calls from originating on and passing through our network. This document delineates Data@ccess's gateway-specific RMP, in addition to related robocall mitigation procedures. Data@ccess is fully STIR/SKHAKEN compliant as an originating VSP. This RMP concerns how Data@ccess handles foreign traffic when it traverses Data@ccess's network.

Know Your Upstream Provider

Section 64.1200(n) of the Commission's Rules³ requires gateway providers to comply with the Commission's "know your upstream provider" requirements. As an initial matter, as described below, Data@ccess has implemented "know your customer" and specific reasonable steps including traffic monitoring to mitigate the risk that it may inadvertently carry or process illegal robocalls on behalf of any of its customers, whether retail end users or wholesale carriers, foreign or domestic.

¹ 47 C.F.R. § 64.6305(b).

² See *In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls Call Authentication Trust Anchor*, Sixth Report and Order in GC Docket No. 17-59, FCC 22-37 (rel. May 20, 2022) at ¶¶ 36-37.

³ 47 C.F.R. § 64.1200(n).

Data@ccess follows procedures to ensure that it knows the identities of all its upstream carriers from which it accepts traffic. To the extent that Data@ccess were to receive information from law enforcement or other sources that a customer is engaged in illegal robocalling, our policy is to cooperate fully, including providing the identity of any suspected illegal robocaller, pursuant to legal service or process. As delineated below, Data@ccess's Acceptable Use Policy gives Data@ccess the right to terminate service in the event customers are making illegal calls.

For all upstream carriers from which Data@ccess accepts traffic, both foreign and domestic, Data@ccess has procedures to monitor incoming traffic, including traffic it processes as a gateway provider, to identify potentially illegal robocalls. This is described in the Monitoring section below. Moreover, Data@ccess's service agreements with all its upstream carriers, foreign and domestic, provide that those carriers will manage intermediate numbers provided to Data@ccess to ensure compliance with FCC regulations and other applicable laws and will work with Data@ccess on such matters.

The accurate identification of a subscriber in the STIR/SHAKEN ecosystem is tied to a telephone number-based caller identity associated that subscriber. A subscriber is an entity that has a business relationship with Data@ccess in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

New Subscribers

All new subscribers go through identity verification protocols which are a mixture of algorithmic check and manual call back. A risk score is developed to ensure the authenticity of a new subscriber. This score checks the identity marker collected during an account registration process. These include but are not limited to: name, email address, credit card information and contact phone number.

These identity markers are validated for accuracy against public and paid tools. All new subscriber activity is monitored as further explained below.

Existing Subscribers

Data@ccess require updates of subscribers' information on all their orders. Each order's identity markers are verified again to ensure the account is not compromised and is being used for its intended purpose.

Acceptable Use Policy

Data@ccess maintains an Acceptable Use Policy ("AUP") that subscribers must sign before being permitted to use Data@ccess's network. Among other things, this AUP prohibits:

- providing altered, deceptive, or false information about the identity of the sender or the origin of a message or phone call;
- violating any applicable local, state, or federal law;
- violating applicable industry accepted guidelines; and
- using Data@ccess's service to engage in or in connection with fraudulent activities.

Data@ccess's contractual terms with subscribers specify that Data@ccess may take action up to suspension or termination of service for violation of the AUP.

Telephone Number Authorization

A Telephone Number ("TN")-based caller identity is the originating phone number included in call signaling used to identify the caller for screening purposes that is uniquely associated with the subscriber. A subscriber is permitted to use a TN as a caller identity if a TN is directly managed by Data@ccess and/or obtained by Data@ccess from one of Data@ccess's underlying carriers for use by the subscriber. In most cases, Data@ccess directly manages the TNs used by its subscribers. Data@ccess tracks these numbers in its inventory system and monitors the assignment of these numbers. In these cases, TN validation is the inherent result of Data@ccess's assignment of the TN to its subscriber.

If a subscriber wishes to use a TN as a caller identity and that TN is not directly managed by Data@ccess, then TN validation is necessary. If a subscriber's end-user can provide a valid letter of authorization that they are the authorized user of such TNs, Data@ccess will attest calls originated with these TNs.

When originating a call, Data@ccess checks the calling party number against Data@ccess's inventory and will not attest the call unless the calling party number is a TN that has been properly validated.

Mitigation Through Contracts

All subscribers agree to participate in traceback requests (this is part of the Terms and Conditions which users must agree to when creating an account with us).

During Service

All subscribers can report any suspicious call connected through their account and measures are set to prevent future calls from/to that individual numbers for all subscribers (none routed by the platform from that moment on - blacklisting). These features include requiring authentication to initiate any call, or a whitelist of originating numbers that is under customer's control.

Monitoring

Data@ccess has a monitoring and reporting system in place to analyze high-volume voice traffic to identify and monitor patterns consistent with robocalls. Our server-based monitoring system alerts us to calling patterns with unusual spikes, traffic patterns, or attempted use of non-validated ANIs to detect patterns consistent with illegal robocalls.

If Data@ccess detects a calling pattern consistent with illegal robocalls, we will identify the party that is using our network to originate those calls and will take appropriate action. Taking appropriate action may include, but is not limited to, initiating a traceback investigation, verifying that the originating subscriber owns or is authorized to use the Caller ID number, and suspending or terminating the party's ability to originate calls on our network.

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, our risk prevention team is alerted which follows the defined procedures on investigating such subscribers.

The procedures established include but are not limited to:

- checking recent and past call detail records and benchmark against expected trends;
- checking recent and past account activity and purchases;
- investigating if any system issue generates the strange behavior;
- verifying that the call originating path is valid; and
- contacting the subscriber to understand his particular use case and validate that the activity belongs to that subscriber.

Data@ccess follows Industry Traceback Group (“ITG”)-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, Data@ccess will devote sufficient resources to provide prompt and complete resources to traceback requests. **Data@ccess certifies that it will comply with traceback requests within 24 hours of receiving same.**

Data@ccess will investigate suspicious activity found by its monitoring systems or reported to Data@ccess by subscribers or third parties. The investigation could potentially result in opening a traceback request or with Data@ccess contacting a subscriber to correct improper use of the platform, or, if the subscriber does not respond or comply, to block their use of the platform.

For all new and renegotiated Data@ccess contracts governing the transport of voice calls, Data@ccess will use best efforts to contractually require Data@ccess’s subscribers to cooperate in traceback investigations by identifying the upstream provider from which the suspected illegal robocall entered our network.

Blocking

Data@ccess will implement Do Not Originate requests it receives from the ITG. Data@ccess has mechanisms to automatically block suspicious calls using internal analytics. If Data@ccess’s monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, Data@ccess will take appropriate action which may include suspending or terminating the subscriber’s use of Data@ccess’s network. Data@ccess will cooperate with Investigative Bodies (provide a single point of contact to address traceback requests from law enforcement (including state attorneys general offices), to the FCC, and/or the ITG; as well as documenting requests & actions taken in response thereto.

Plan Updates

This plan and industry best practices must evolve to response to the dynamic nature of mitigating illegal robocalling. Data@ccess will monitor industry best practices and continuously improve our internal processes to ensure this plan and our system adapt to this ever-changing issue.

In the event of any material change to this plan, Data@ccess will republish it to employees, consultants and contractors and file such an update to the FCC Robocall Mitigation Database within ten (10) days of such update.