

1stel Robocall Mitigation Program

Robocall Mitigation

All customers have agreed and are subject to 1stel, Inc. [AUP](#) .

1stel, Inc. implements a proprietary analytic application that monitors and alerts of suspicious activity resulting in an investigation and suspension of service, until corrective action is taken.

1stel, Inc. by default implements all non-NANPA call barring. Customers that require non-NANPA are required to sign a responsibility agreement for the calls they originate.

1stel, Inc. cooperates with the upstream providers with regards to suspicious activity.

Know your customer

1stel, Inc. takes the following steps to prevent new and existing customers from originating robocalls:

- Our customers are small businesses only and have disclosed full contact information, and 1stel validates the business identity and physical location of voice services.
- Telecom interconnections are based on an “Allow Specific, Deny All” control list policy.
- VOIP connections are based on Caller ID Authentication and “Allow Specific, Deny All” control list policy
- Our contractual provisions prevent customers from originating illegal robocalls. If illegal activity is detected the customer will be warned and disconnected if activity continues.

Know your upstream provider

1stel, Inc. receives its upstream traffic from two US-based carriers. We have reviewed the RMP of both carriers to verify their methodology of monitoring for illegal robocalls and that they implement DNO blocking as required.

1stel, Inc. does not directly receive voice traffic from any foreign originating or intermediate carrier.

Traceback

1stel, Inc. will cooperate with all Traceback requests from the Commission, law enforcement, and the registered traceback consortium.

Principals, Affiliates, Subsidiaries, and Parent Companies

Directors

Nathan Bowyer

Ryan Bowyer

Douglas Bowyer

Sherry Bowyer

Kelsie Gonzalez

1stel, Inc. has no subsidiaries or parent companies, and does not offer voice services through affiliates.