

Direct Telco LLC

ROBOCALL MITIGATION ACTION PLAN

A. KYC Process

We take the KYC procedure very seriously at Direct Telco LLC. Each client is required to sign the subsequent agreement and provide supporting documentation from the list below.

Master Service Agreement

Legitimate traffic disclaimer form

KYC Form Company Registration Certificate

Permanent Address Proof

FCC499A Filer ID

Last 12 months Trace Back portal data

Supporting Document List

B. Fraud Filter on Traffic Origination

Each client trunks at Direct Telco LLC

is subjected to the following filter, and we employ 46 Labs to ensure 100% accuracy.

- 2. DNC
- 2. DNO
- 2. ANI Filter
- 2. DNIS Validation

- 2. Cell ANI Reject
- 2. Neighborhood Spoofing
- 2. 404

C. Trace Back Response

Depending on the specifics of the issue, Direct Telco LLC tries to reply to traceback requests between 4 hours and 24 hours.

The majority of tracebacks receive a response in less than four hours, however we have a 24-hour maximum for any given circumstance.

D. STIR-SHAKEN IMPLEMENTATION STATUS

Direct Telco LLC only processes USA traffic that is verified with a Stir/Shaken token. We do not accept traffic from customers who do not sign their own traffic. In addition, the Provider has established the policies and procedures set forth in this Robocall Mitigation Plan which are intended to stop anyone from using the Provider's service to originate illegal robocalls.

I CUSTOMER VETTING PRACTICES

As a means of preventing or minimizing the origination of illegal robocalls through its voice services, the Provider will use best practices in vetting the identity of all of its voice service subscribers, whether a retail or business/commercial subscriber (including any entities that are purchasing the Provider's services for resale). The subscriber vetting process is intended to help determine the legitimacy of a customer for the purpose of establishing a business relationship. Generally, the Provider looks to confirm the identity of customers using their voice services through collecting information such as physical customer location, contact person(s), state or country of incorporation, federal tax ID, and the nature of the customer's business. Provider efforts to vet retail and business/commercial subscribers occur during the process of provisioning customer requested services (for example in appropriately sizing the facilities to their claimed intended use), executing the Provider's required service agreements, and granting the customer the right to use telephone number resources. Commercial end users, comprised of larger businesses with more complex service configurations, are generally recognized as presenting a higher risk of perpetrating illegal robocalls and thus those customers, at the Provider's discretion, may be subject to an additional review, including a more stringent background check and possibly a site visit. The Provider also understands the special importance of vetting any

wholesale customers it may have. If necessary, the Provider may vet identity information for its wholesale customers by confirming whether the customer is an FCC Form 499-A filer in the FCC Form 499-A Filer database or in the FCC's Intermediate Provider Registry. If the customer is not registered within those databases further investigation is conducted to better understand the nature of the customer's business.

Further, with respect to meeting existing obligations to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls, the Provider:

Utilizes service agreements and acceptable use policies as a means of preventing its new and existing subscribers from using their voice and broadband services in ways that would be in violation of local, state, or federal laws, or to engage in deceptive or fraudulent activity. These documents governing use of Provider provided services include terms indicating specifically to all customers that their services should not be used for the purpose of making illegal robocalls, and the Provider reserves authority within its service agreements to suspend or terminate a subscriber's voice service for violating applicable service-related terms.

- Has established a routine process for monitoring the usage and quality of its network facilities and conducts recurring and timely reviews of its call detail records (CDRs) to facilitate early identification of unusual or suspicious calling activity or
- those instances where the Provider identifies activity or a pattern consistent with illegal robocalls the customer will be contacted within 24 hours for further investigation and possible action regarding their subscribed to voice service.

I E. THIRD-PARTY CALL ANALYTICS

Direct Telco LLC is also testing several third-party call analytics to further assist and prevent origination of illegal robocalls on its network. These call analytics system(s) used to identify and block illegal robocall traffic.