

Robocall Mitigation Plan

Red Cloud LLC has not been prohibited from filing a certification in the Robocall Mitigation Database. Neither Red Cloud LLC, nor any of our executives or principals, have a history of enforcement actions for illegal robocalls, TCPA or TSR violations, or related state law violations. We use the affirmative and effective measures detailed below to prevent the origination or transit of illegal robocalls:

Know Your Customer

We follow the caller ID authentication best practices for vetting caller identity and operational legitimacy for new and existing customers as described by the NANC Call Authentication Trust Anchor Working Group.

The following information is collected from our customers during the standard onboarding process:

- Name
- Federal taxpayer ID
- Physical and mailing addresses
- Contact telephone numbers
- Email addresses of principals and controlling persons of the entity
- Any persons with a majority ownership interest in the customer
- Staff responsible for compliance with TCPA, TSR, and other such laws

For those involved in telemarketing, we additionally collect the customer's Do Not Call Registry subscription account number, Universal Service Fund registration number, a copy of their FCC 499, and Section 214 International Authority (if applicable).

Our process includes the collection and review of entity-identifying information to confirm that we have an authenticated relationship with the customer. We use this authenticated information to determine whether the customer is subject to any enforcement actions that restrict the type of calling that they may do, for example, if they have been banned from initiating telemarketing calls.

We also validate, when possible, that the entity has a legitimate right to use its asserted calling numbers. We use this information to support the attestation level we assign to calls that we originate for that customer.

Our contractual provisions with customers prohibit them from initiating

illegal robocalls. If we find a customer initiating suspicious robocalls, we warn them to stop. If such traffic continues, we then terminate their service.

Traceback

We respond to all traceback requests from the Commission, law enforcement, and the registered traceback consortium within 24 hours and cooperate fully with such entities in investigating and stopping any illegal robocallers that use our service to originate calls.

Robocall Mitigation Program

We use call analytics software provided by True IP Solutions to monitor all outbound voice traffic in real-time to prevent the origination or transit of illegal robocalls. This software provides detailed reporting to identify suspected illegal robocalls. The system blocks and alerts us if we process outbound calls whereby the calling number has a poor reputation or is invalid, unallocated, or on a Do Not Originate list.

As permitted by FCC 47 CFR 64.1200(k), we block a call when an originating number is malformed, unallocated, on a Do Not Originate list, and/or analytics software or prior activity indicates the call is likely an illegal robocall. As required by this federal regulation, we provide our customers information on how to opt out of call blocking (47 CFR 64.1200(k)(3)(iii)).

We immediately investigate any identified suspicious calls to determine if the caller was attempting to originate or transit unlawful robocalls. If we determine that the traffic was likely unlawful, we warn them to stop sending such traffic. If they continue to send traffic that appears to be unlawful, we terminate their service.

There is also a periodic manual review of blocked calls to ensure previous call blocking was proper and act accordingly if, after investigation, it's found the blocking was erroneous, as required by the FCC Fourth Report and Order in the matter of "Advanced Methods to Target and Eliminate Unlawful Robocalls" (FCC 20-187).

We are prepared to block calls or terminate service from any customer or source if asked to do so by the FCC. We rely on our voice origination carriers to follow all common sense and FCC requirements and only accept traffic from providers with an RMD filing, as required by 47 CFR 64.6305(d).

STIR/SHAKEN

We have fully implemented STIR/SHAKEN across our network in accordance with FCC requirements. All calls we originate are signed with appropriate attestation levels, ensuring caller identity can be validated by downstream providers.