

Rmtel Networks LLC Robocall Mitigation Policies

New and Renewing Customers:

Collect the following information from new customers:

Business name, Contact name, Business service address, ISP, Numbers to be ported and hosted, losing LEC, Services requested.

Verify ownership of the numbers and a customer's right to use the number by requiring a bill dated within the last 30 days from the customer's losing LEC that includes the numbers to be ported and the account number of the losing LEC and the service address.

Services are month to month with no contracts.

All seats, trunks, and services are restricted to 5000 minutes per month.

Services requiring more outbound minutes than 5000 per month are to be metered, monitored, and individually verified weekly.

Customer's BBB rating, public legal records, and local reputation are considered for each new customer onboarded. These records are to be reviewed annually on the anniversary of the initiation of service.

Measures that Rmtel Networks LLC employs to avoid the origination of illegal robocalls include:

1. Customers who exceed the 5000 minute limitation more than once per quarter or who's records indicate large quantities of short duration calls or calls to sequential numbers will be investigated and their service suspended or cancelled.
2. Currently, CDR records are hand verified, but software analytics should be implemented in the future.
3. Customers may only use outbound caller ID for numbers that they own and are able to legally use. Blind caller ID, caller ID masking, and caller ID spoofing are not allowed and service will be terminated immediately if these restrictions are bypassed or hacked. This should not be possible since these requirements are coded into the server side, which means that if it does happen for any reason it will be grounds for immediate cancellation of service.
4. Currently, there are no measure in place to automatically block incoming calls. This will be examined and addressed in the future.

There are financial penalties in place for the customer who initially breaks these policies. If the customer consistently breaks these policies (exceeding 3 times), their service may be suspended and cancelled. There must be an investigation to determine why their usage is outside of the normal range. If it is for legitimate usage, then the server must be programmed to allow for their service needs.

Responding to Traceback Requests

If a customer originates a call or series of calls that is the subject of a traceback request or a large volume of traceback requests, then their service will be cancelled.

If a customer is identified by the FCC as originating illegal calls, then their services will be immediately cancelled and the information will be provided to law enforcement as requested or required.