

Outpost Labs Inc. dba Trellus AI ("Trellus") submits the following Robocall Mitigation Plan ("RMP") as regards customers and traffic for which its upstream partners deem it to be a Voice Service Provider. Trellus originates outbound voice traffic solely through upstream carrier partners Twilio Inc and Bandwidth Inc, and as such Trellus does not operate its own transmission facilities nor does Trellus have any STIR/SHAKEN implementation obligations.

Trellus certifies that it commits and responds within 24 hours to all traceback requests from the Commission, law enforcement, and the Industry Traceback Group as designated by the Federal Communications Commission ("FCC") pursuant to 47 C.F.R. § 64.1203, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

Business Information:

Business Name: Outpost Labs Inc. (dba Trellus AI)

Business Address: 169 Madison Ave #2457, New York NY 10016

RMP Owner: Craig Bonnoit, Co-Founder

Compliance Lead: Craig Bonnoit, Co-Founder

Compliance Lead Contact: craig@trellus.ai, 16175124786

STIR/SHAKEN Implementation.

Trellus certifies and acknowledges it has not implemented the STIR/SHAKEN authentication framework on any portion of its network. Trellus does not have control over the infrastructure required for STIR/SHAKEN implementation per § 64.6305(d)(2)(i). Therefore, Trellus does not directly sign calls. However, Trellus does certify the following:

1. Trellus routes all outbound traffic through its upstream providers, Twilio Inc (FCC Registration Number: 00200237343) and Bandwidth Inc. (FCC Registration Number: 0015443773) (collectively, "Upstream Providers").
2. The Upstream Providers have represented to Trellus that they implement STIR/SHAKEN authentication in accordance with FCC requirements. Trellus has verified their RMP filings also state they are in accordance with STIR/SHAKEN guidelines.
3. Trellus assigns and manages telephone numbers through its upstream providers.
4. Trellus customers are only allowed to transmit calls with numbers they own as registered and enforced by upstream providers through voice API services.
5. Trellus requires customers to only use telephone numbers that are either (a) assigned by Trellus or (b) properly ported into a compliant upstream provider who have filed with the Robocall Mitigation Database with provider verified authorization.

Contractual Protections

All Trellus customers are required to contractually commit to lawful use of Trellus services. This includes prohibition on using or directing Trellus to make:

1. outbound calling without proper consent or exceeding federal or state guidelines on allowed calling
2. prerecorded voice calls without proper consent in violation of law
3. automated dialing in violation of TCPA

4. any unlawful telemarketing activity
5. scams, impersonation, or fraudulent schemes

Know Your Customer Practices

Trellus employs a layered and risk based approach to identity verification.

1. All users are restricted in their ability to originate calls on a per-user per-day basis.
2. Customers are additionally restricted in total weekly calling.
3. All customers using texting must go through A2P campaign screening conducted by an upstream carrier.
4. Depending on customer risk profile, origination volume, and upstream carrier, customers may be required to provide the following additional information:
 - a. Business entity identification (Legal name, address, EIN)
 - b. Principal identification (Name, address, email, phone number)
 - c. Payment credentials (name, card number, expiration date, CVC, billing address, and ZIP code)
 - d. Use case documentation
 - e. Acknowledgement and acceptance of consent-based limitation on use
5. Where applicable, credit card processing is completed through Stripe which also employs anti-fraud measures.

Monitoring & Manual Review

1. Trellus's primary defense is limitations on outbound call origination per user per day.
2. Trellus additionally conducts automated screens for (a) customers with high short duration calls, (b) customers with high invalid destinations, and (c) customers with frequent high risk conversations including account / identity numbers, suspicious payments, or scam accusations. Accounts triggering these screens are subject to a manual review.
3. Trellus additionally may conduct manual vetting on teams with high origination volumes.
4. Trellus additionally conducts a manual review of traffic in response to all consumer complaints.
5. Manual reviews may result in customer warnings, additional limitation on outbound activity, or account closure.

Ongoing Compliance Obligations

Trellus is aware of its ongoing compliance obligations including, but not necessarily limited to, the following:

1. Trellus will ensure the annual recertification of this RMP will be completed by March 1 each year
2. Trellus will ensure this RMP is updated within 10 business days for any required updates or changes to submitted information
3. Trellus will ensure all FCC investigations, FCC requests, and/or FCC Enforcement Bureau blocking directives will be met in a timely manner.

Fraud and Compliance Team

Trellus's leadership team is responsible for reviewing alerts and overseeing all manual reviews. Trellus's leadership team will additionally coordinate with upstream carriers to investigate suspected illegal robocall traffic, identify originating customers, enforce carrier-level requirements, and comply with mitigation directives.