

ROBOCALL MITIGATION PLAN

This Robocall Mitigation Plan (“RMP”) describes: (1) the specific reasonable steps we have taken to avoid carrying or processing illegal robocall traffic; (2) our commitment to respond fully and within 24 hours to all traceback requests from the Federal Communications Commission (“Commission”), law enforcement, and the industry traceback consortium; and (3) our commitment to cooperate with such entities in investigating and stopping any illegal robocallers that use our services to carry or process calls.

I. ENTITIES COVERED BY CERTIFICATION

The following entities are all subject to the robocall mitigation policies and procedures described in this RMP:

- Ooma, Inc. (FRN: 0017027111)
- Junction Networks Inc. (FRN: 0021330824)
- Broadsmart Global, Inc. (FRN: 0025715012)
- Voxter Communications Inc. (FRN: 0028440600)
- 2600hz, Inc. (FRN: 0022722623)
- Talkatone, LLC (FRN: 0023473408)
- FluentStream Technologies, LLC (FRN: 0022369417)
- Phone.Com, Inc. (FRN: 0016845190)

Ooma, Inc. is the direct or indirect parent of each of the other entities listed above, and all of these entities are subject to this RMP. For the purposes of this RMP, these entities are collectively referred to as “Ooma.”

II. DESCRIPTION OF ROBOCALL MITIGATION PLAN

A. Efforts to Avoid Carrying or Processing Illegal Robocalls

Ooma has made investments to combat carrying or processing illegal robocalls. Ooma engages in, or is working on implementing, the following practices to help minimize the impact of illegal or unwanted robocalls on customers:

- **Know Your Upstream Provider:** Knowledge of carriers from which we receive traffic and review of whether such carriers are listed in the Robocall Mitigation Database. Ooma has also reviewed any carrier’s RMPs to learn how the carriers monitor their originating traffic to mitigate illegal robocalls.
- **Know Your Customer:** Ooma investigates prospective customers’ information, which may include information such as email address, mobile phone number, service location, IP address validation, CAPTCHA challenges, mobile app attestation, and in the case of business customers, additional information such as business website, business registration details, credit application, and past robocall violation reports. Business customers reselling

certain of our services who are classified by the FCC as providers are subject to an enhanced vetting process, which may include review of their FRN, 499 and robocall mitigation database filings.

- **Robocall Mitigation Program:** Monitoring of outbound voice traffic to help prevent the origination of illegal robocalls. Combining behavioral analytics, caller authentication and verification, the monitoring may feature:
 - Fraud Detection: Detection of high-volume robocalling, spoofing, spam call activity, traffic pumping activity (e.g., high number of minutes to high-cost destinations), high volume of international calls, high volume of domestic calls, and account log-in failures.
 - Subscriber Notification: Customer Support notifications of suspect activity to warn subscribers of suspicious calls.
 - Call Blocking Support: Identification of and enabling end users to block fraudulent phone calls, including using custom and industry available databases for number validation.
 - Business Number Verification: Register legitimate business numbers to prevent unintentional call blocking.
 - Caller ID Name Service: Integration of Caller ID name lookup service, including robocall mitigation with override to include original caller ID even when call is determined fraudulent.
 - Credit Card and Customer Validation: Suspension of fraudulent customers when they match known invalid credit card or other fraud patterns, such as payment failures at the beginning of the customer cycle.
- **Contract Termination:** Ooma typically has contractual rights that allow it to terminate customers that violate relevant law, including violation of the Telephone Consumer Protection Act. When appropriate, Ooma enforces these rights. Subject to applicable laws that may prevent it from doing so, Ooma may also terminate accounts if it discovers that any of the entities or individuals associated with a customer account have been named by the Commission or the Federal Trade Commission (“FTC”) as an illegal robocaller or have failed to respond to traceback requests.

B. Traceback Requests

Ooma commits to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium.

C. Commitment to Cooperate in Investigating and Stopping Illegal Robocallers

Ooma also promptly responds to inquiries from law enforcement and regulators, including the Commission, FTC or state attorneys general seeking traceback or similar information. Ooma commits to continue to cooperate with the Commission, law enforcement, and the industry traceback consortium in investigating and stopping any illegal robocallers that use Ooma’s services to carry or process calls.

D. STIR/SHAKEN Compliance

Ooma has implemented STIR/SHAKEN to all egress traffic. STIR/SHAKEN uses digital certificates, based on common public key cryptography techniques, to ensure the calling number of a telephone call is secure. The expectation is that the certificate technology will enable the called party to verify that the calling number is accurate and that it has not been spoofed.