

Acceptable Use Policy

Last Updated: July 12, 2026 · Version 1.0 | FRN 0038523411 · OCN 417M

1. Introduction and Acceptance

This Acceptable Use Policy ("Policy" or "AUP") governs the use of all voice and related services ("Services") provided by Best VoIP Dialer LLC (the "Company"). This Policy is incorporated by reference into the Company's Master Service Agreement, and every customer — and any party using the Services through a customer ("Customer") — agrees to comply with it as a condition of service. Use of the Services constitutes acceptance of this Policy.

2. Compliance with Law

Customers must use the Services in full compliance with all applicable federal, state, and local laws and regulations of the United States and of any jurisdiction from which or into which calls are placed, including without limitation: the Telephone Consumer Protection Act (TCPA), 47 U.S.C. § 227, and the FCC's implementing rules, 47 C.F.R. § 64.1200; the FTC Telemarketing Sales Rule, 16 C.F.R. Part 310; the Truth in Caller ID Act, 47 U.S.C. § 227(e); federal and state Do-Not-Call statutes and registries; the TRACED Act and FCC rules relating to STIR/SHAKEN and robocall mitigation, including 47 C.F.R. § 64.6305; and, where applicable, the CAN-SPAM Act, 15 U.S.C. § 7701 et seq.

3. Prohibited Activities

Customers may not use the Services, directly or indirectly, to:

- (a) place, originate, or facilitate illegal robocalls, or any call made without consent required by law;
- (b) transmit false, misleading, or inaccurate caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value ("spoofing");
- (c) place calls to numbers on the National Do-Not-Call Registry, any state do-not-call registry, or a called party's entity-specific do-not-call list, except as permitted by law;
- (d) use an automatic telephone dialing system or artificial/prerecorded voice messages without the prior express written consent of the called party where such consent is required;
- (e) engage in fraud, identity theft, phishing or vishing, deceptive marketing, impersonation of government agencies or businesses, or collection of information under false pretenses;
- (f) harass, threaten, abuse, or intimidate any call recipient, or continue calling a number after a request to stop;
- (g) engage in traffic pumping, access stimulation, toll fraud, call looping, or any scheme designed to generate artificial traffic or improper intercarrier compensation;
- (h) interfere with, disrupt, or attempt to gain unauthorized access to the Company's network or systems, or the services of any third party; or
- (i) resell or transit third-party traffic over the Services without the Company's prior written approval and completion of the Company's wholesale onboarding and verification requirements.

4. Telemarketing and Autodialed Traffic Requirements

Customers conducting telemarketing or transmitting autodialed traffic must, at minimum:

- (a) maintain an active subscription to the National Do-Not-Call Registry and scrub all calling lists against the federal registry, applicable state registries, and their internal do-not-call list before dialing;
- (b) scrub calling lists against the FCC Reassigned Numbers Database or an equivalent verification source;
- (c) obtain, retain, and produce upon request evidence of the prior express written consent of each called party where required, including lead-generation consent records (e.g., TrustedForm or Jornaya certificates);
- (d) honor opt-out and do-not-call requests immediately, and in all events within the period required by law;
- (e) restrict calls to between 8:00 a.m. and 9:00 p.m. local time at the called party's location;
- (f) transmit accurate caller ID and display a number that is answered and identifies the calling party on callback; and
- (g) provide, upon the Company's request, the identity of the entity on whose behalf calls are made, sample scripts or recordings, the ANIs in use, campaign volumes and dates, and proof of the foregoing compliance measures.

5. Caller ID and Number Use

Customers may originate traffic only from numbers assigned by the Company or from numbers the Customer is verifiably authorized to use. The Company validates ANIs against assigned and verified ranges; unverified numbers are blocked. Use of wireless numbers as caller ID is restricted unless authorized. Calling patterns consistent with neighborhood spoofing, or caller ID rotation designed to evade identification, are prohibited.

6. Traffic Quality

Traffic must reflect legitimate business calling. The Company continuously reviews traffic metrics — including answer-seizure ratio, average call duration, call velocity, and complaint and reputation data — and may investigate, restrict, or block traffic whose profile indicates abusive, artificial, or illegal calling.

7. Monitoring and Enforcement

The Company monitors traffic in real time and applies layered filtering as described in its Robocall Mitigation Program, including Do-Not-Originate lists, blocking of invalid or unallocated numbers, destination validation, and reputation-based signals. Suspected illegal traffic may be blocked pending investigation. Violations of this Policy may result, at the Company's sole discretion and in accordance with its graduated enforcement process, in required list remediation and re-scrubbing; capacity restriction; blocking of specific numbers or destinations; suspension of service; or immediate termination. The Company maintains a zero-tolerance policy toward illegal robocalling and may act immediately and without prior notice where the severity, willfulness, or volume of traffic warrants. Each investigation, determination, and action taken is documented, and the Company may notify upstream or downstream providers and regulators as appropriate.

8. Traceback and Investigations

Customers must cooperate fully with any inquiry, investigation, or traceback request initiated by the Company, the FCC, the FTC, state attorneys general, law enforcement, or the Industry Traceback Group, and must respond to the Company's requests for information promptly — and in every case within twenty-four (24) hours. Failure to respond or cooperate is grounds for suspension or termination of service.

9. Records

Customers must retain records sufficient to demonstrate compliance with this Policy — including consent evidence, scrub logs, and campaign documentation — for a minimum of two (2) years, and must produce such records to the Company upon request.

10. Reporting Violations

Suspected violations of this Policy may be reported to the Company's compliance team at compliance@bestvoipdialer.com. Reports are reviewed promptly and investigated in accordance with the Company's Robocall Mitigation Program.

11. Changes to this Policy

The Company may modify this Policy at any time to reflect changes in law, regulation, or its operations. The current version is maintained at <https://bestvoipdialer.com/legal/aup.pdf>, and continued use of the Services after an update constitutes acceptance of the revised Policy.

12. Contact

Best VoIP Dialer LLC

11425 Hufsmith Kuykendahl Road, Tomball, Texas 77375

compliance@bestvoipdialer.com · <https://bestvoipdialer.com>

FRN: 0038523411 · OCN: 417M