

UnlimCall Robocall Mitigation Plan

Submitted in accordance with the TRACED Act and 47 CFR § 64.6305(c) for filing in the FCC Robocall Mitigation Database.

Legal Entity: UnlimCall LLC (Delaware)

Effective Date: June 11, 2026

Version: 1.2

1. Executive Summary

UnlimCall LLC is committed to preventing the origination and transmission of illegal robocalls across its voice network and to protecting the integrity of the calls its customers place. This Robocall Mitigation Plan describes the specific, technical, and procedural measures UnlimCall has implemented to stop unlawful and abusive calling at its source, consistent with the TRACED Act and the Federal Communications Commission's robocall mitigation rules. UnlimCall files this plan as part of its certification in the FCC Robocall Mitigation Database (RMD).

UnlimCall is a business-to-business voice carrier that gives outbound call centers real, locally allocated phone numbers in 33 countries and bills them at a flat per-agent rate rather than per minute. While flat-rate billing is a commercial feature, UnlimCall does not treat it as a compliance control; rather, it structurally offsets the volume risk traditionally associated with flat-rate dialing through architectural mitigation at the network layer. Every call must originate on a genuine in-country number allocated under UnlimCall's own local authorization — not on a faked foreign number or a neighbor-spoofed caller ID — which removes the single most common vector for illegal caller-ID manipulation; and concurrency is capped at one call per line, so that no single credential can produce a mass-dialing spike. On top of this network, UnlimCall combines authenticated call signing, manual Know-Your-Customer (KYC) vetting with enhanced diligence for high-risk verticals, real-time heuristic traffic analysis, and rapid traceback response.

UnlimCall is an authorized STIR/SHAKEN service provider. It signs every eligible United States and Canadian outbound call with full "A"-level attestation, holds its own Service Provider Code (SPC) token, and is listed in the FCC Robocall Mitigation Database. For its international markets, where STIR/SHAKEN does not apply, UnlimCall relies on genuinely allocated in-country numbering under local regulatory authorization as the equivalent caller-identity-integrity control. This plan applies uniformly across all UnlimCall services — SIP trunking for bring-your-own-dialer call centers, hosted auto-dialing, AI voice agents, AI receptionist, and number provisioning — and to both outbound and inbound traffic on the network.

The sections that follow set out UnlimCall's corporate compliance framework, the scope of its services and provider role, its STIR/SHAKEN status, its caller-ID authentication and number-validation controls, its KYC and vetting protocols, its real-time monitoring and analytics, its inbound and outbound mitigation practices, its traceback cooperation and enforcement procedures, its data retention and audit practices, and the obligations imposed on its customers.

Together these measures demonstrate UnlimCall's commitment to lawful, reputation-protective operation of its network.

2. Corporate Compliance Framework

UnlimCall operates under a stated zero-tolerance policy toward illegal robocalling and SPAM, enforced through its Acceptable Use Policy (AUP) and Master Service Agreement. Protecting the reputation of its network — and the local number pools its customers depend on — is treated as a core operating priority rather than an afterthought, because a network that tolerates abuse degrades answer rates and caller-ID trust for every legitimate customer on it.

UnlimCall's compliance posture is proactive. It maintains current STIR/SHAKEN authorization, TLS 1.2+ signaling encryption and SRTP media encryption on by default, GDPR-aligned EU-resident data handling, and a manual KYC program. A SOC 2 Type II audit is in progress and an attestation letter is available on request; ISO 27001 control alignment is underway with certification scoped for 2027. UnlimCall does not represent controls as complete before they are, and this plan describes only measures that are live unless explicitly identified as roadmap items.

Responsibility for robocall mitigation is shared across the organization, from leadership through network engineering and the Network Operations Center (NOC). Internal policies prohibit any use of UnlimCall services for illegal, fraudulent, deceptive, or abusive communications, and they bind customers, resellers, and interconnect partners alike. Where indications of non-compliance arise, UnlimCall investigates promptly and is empowered under its AUP to suspend or terminate offending traffic without prior notice. UnlimCall treats applicable legal frameworks — including the TRACED Act, the Telephone Consumer Protection Act (TCPA), the Telemarketing Sales Rule, FCC Truth-in-Caller-ID rules, and, for its international footprint, the corresponding local consumer-protection and numbering regulations — as the baseline standard of conduct on its network.

3. Scope of Services and Provider Role

Provider Role. UnlimCall operates principally as an *originating voice service provider*: it provides telephone numbers and outbound calling service directly to its business customers and signs their eligible US/CA calls under its own STIR/SHAKEN credentials. UnlimCall also *terminates* inbound calls to numbers it hosts (for example, calls delivered to its AI receptionist and DID customers). To the extent UnlimCall ever carries traffic in an intermediate capacity, the same authentication, vetting, and monitoring controls described in this plan apply. UnlimCall does not operate as an open wholesale transit hub and does not knowingly carry traffic for non-compliant upstream providers.

Service Offerings. UnlimCall's robocall mitigation controls apply uniformly across the following services:

- **Flat-rate SIP trunking (BYOD):** Standard SIP credentials (host, username, password, codec list) over UDP/TCP/TLS for call centers running their own dialers — for example ViciDial, GoHighLevel, FreePBX, Asterisk, FreeSWITCH, and standard softphones. Concurrency is enforced at one concurrent call per line on the network.

- **Local number provisioning:** Real, in-country DIDs allocated under UnlimCall's local authorizations across 33 countries in North America, Western, Central, Eastern, Northern and Southern Europe, and Asia-Pacific, used as authenticated outbound caller ID.
- **Hosted auto-dialer:** Predictive, power, preview, and progressive dialing on the UnlimCall trunk, subject to pacing, concurrency, and consent controls. Because the network enforces a strict one-call-per-line capacity limit (Section 7), a customer running predictive dialing must provision multiple concurrent lines per agent seat to achieve a given dialer ratio; the maximum dialer ratio is therefore bounded by the number of lines the customer provisions and is visible to UnlimCall, rather than being unconstrained.
- **AI voice agents and AI receptionist:** Autonomous outbound voice agents and 24/7 inbound answering, both operated within the same caller-ID authentication, consent, and monitoring controls applied to human-agent traffic. Outbound AI-voice and voice-cloned calls are additionally subject to the artificial-/prerecorded-voice consent obligations described in Section 11.
- **Voice cloning:** Brand-voice synthesis applied to AI agent calls, subject to the same prohibitions on impersonation and deceptive use set out in the AUP.

Across all of these, UnlimCall's network is fully IP-based. The scope of this plan encompasses all UnlimCall voice traffic, inbound and outbound, across every product line and customer type.

4. STIR/SHAKEN Implementation Status

UnlimCall has fully implemented STIR/SHAKEN call authentication for its United States and Canadian outbound traffic and operates as an authorized signing provider. UnlimCall holds the necessary credentials — including a Service Provider Code (SPC) token and digital certificates obtained through the industry STI ecosystem — and is listed in the FCC Robocall Mitigation Database. Its call signing is designed to satisfy both the FCC mandate and the Canadian CRTC caller-ID authentication requirement.

Attestation policy. Because UnlimCall allocates and controls the numbers its customers dial from, the large majority of its US/CA outbound calls qualify for and are signed at full **“A”-Level (Full) attestation**, which affirms to the terminating carrier that UnlimCall is the originating provider and that the calling party is authorized to use the displayed number. Eligibility for A-Level attestation is conditioned on transmitting calls only from DIDs the customer legally owns or is explicitly authorized to use, and on responding to traceback requests within 24 hours.

UnlimCall does not use attestation downgrade as a means of passing unvalidated end-user traffic. A call that presents a caller ID the originating customer is not authorized to use is **blocked outright at origination** (Section 5) — it is not signed and forwarded. **“B”-Level (Partial) attestation** is applied only where UnlimCall has a verified, direct relationship with the customer but cannot fully confirm the customer's authorization to use a particular presented number. **“C”-Level (Gateway) attestation is not used for UnlimCall's direct end-user origination.** Where a customer repeatedly violates these conditions or fails to respond to a traceback, UnlimCall suspends the account rather than continuing to sign its traffic.

Inbound verification. For inbound calls that carry an Identity header, UnlimCall verifies the STIR/SHAKEN signature and uses the attestation result as an input to call handling. Calls that fail verification or present an untrusted signature are treated as suspect and are subject to heightened scrutiny, labeling, or rejection.

International markets. STIR/SHAKEN is a North American Numbering Plan framework and does not apply outside the US and Canada. In UnlimCall's other markets, the equivalent caller-identity-integrity control is structural: outbound calls originate from genuine numbers allocated in-country under UnlimCall's local authorization and terminate as domestic calls, rather than as foreign numbers forwarded across borders. This both raises legitimate answer rates and removes the cross-border spoofing pattern that local carriers flag as fraud.

5. Caller ID Authentication and Number Validation

Ensuring that caller-ID information is authentic and authorized is central to UnlimCall's robocall mitigation strategy and is reinforced by the structure of its product:

- **Locally allocated numbers, not spoofed numbers.** UnlimCall's core anti-spoofing control is architectural. Customers dial from real numbers that UnlimCall has allocated to them in-country, not from foreign numbers configured to imitate a local presence and not from neighbor-spoofed caller IDs. This removes the most common mechanism of illegal caller-ID manipulation before any per-call check is applied.
- **Authorized-number enforcement.** Each customer may present only caller-ID numbers that UnlimCall has assigned to them or that the customer has demonstrated legal authority to use. Outbound calls are checked against the customer's authorized number set; calls presenting a number outside that set are blocked or held for review. This is also the precondition for A-Level attestation on US/CA traffic.
- **Truth-in-Caller-ID compliance.** UnlimCall's AUP prohibits falsifying, altering, or obscuring caller-ID (ANI) information with intent to defraud, cause harm, or wrongfully obtain anything of value, consistent with the FCC's Truth-in-Caller-ID rules. Customers may not present a number they do not own or have rights to use.
- **Number validation.** UnlimCall applies format and consistency checks to outbound caller IDs (valid NANP and E.164 formatting, allocated and assigned ranges) and rejects malformed or unallocated numbers. For high-volume customers using their own number blocks, UnlimCall may require letter-of-authorization documentation before permitting traffic on those numbers.
- **STIR/SHAKEN signing.** As described in Section 4, eligible US/CA outbound calls are signed with UnlimCall's certificate at the appropriate attestation level, and inbound signed calls are verified. This adds a cryptographic trust layer to the caller ID when interconnecting with other carriers.

These controls collectively ensure that only valid, authorized caller IDs traverse UnlimCall's network, materially reducing the opportunity for spoofing and caller-ID fraud.

6. Know-Your-Customer (KYC) and Vetting Protocols

UnlimCall deliberately verifies customer legitimacy through manual human review rather than relying solely on automated, black-box approval systems. This protects the shared reputation of the network and the customer CLI pools that would otherwise be exposed to another customer's abuse. Key elements of the program include:

- **Business entity verification.** Each customer must establish its legal identity and good standing before provisioning — for example through entity registration documents and verification of the responsible principals. UnlimCall collects the full legal name, physical business address, and responsible-party contact details, and screens against applicable sanctions and watchlists (including OFAC).
- **Use-case and traffic vetting.** UnlimCall assesses each customer's intended use of the service — industry, dialing model, destinations, and expected volumes — against legitimate calling patterns, and requires acceptance of the AUP as a condition of service.
- **Enhanced diligence for high-risk verticals.** UnlimCall openly serves verticals that carry elevated regulatory risk — including Forex, crypto, final expense, solar, merchant cash advance (MCA), real estate, lead generation, and debt collection — and applies heightened, vertical-specific audits to them. Customers in these verticals are subject to closer scrutiny of consent practices, calling lists, and pacing, and may be required to evidence prior express consent and Do-Not-Call (DNC) scrubbing before high-volume campaigns are permitted. UnlimCall declines or restricts service where lawful-use safeguards cannot be demonstrated.
- **AUP acknowledgement.** Every customer accepts UnlimCall's Acceptable Use Policy, which codifies the prohibitions on illegal robocalling, caller-ID spoofing, telemarketing fraud (including tech-support, IRS/tax, and "wangiri" one-ring schemes and vishing), harassment, and toll fraud / artificial inflation of traffic. Acceptance creates a binding obligation enforceable by suspension or termination.
- **Ongoing re-vetting.** Vetting does not end at signup. UnlimCall monitors account behavior on a continuing basis and re-evaluates any customer implicated in robocall complaints, traceback findings, or regulatory action. Customers who fail vetting, provide false information, or are known to have a history of robocall violations are denied or removed.
- **Partner and supplier diligence.** Before exchanging traffic with another provider, UnlimCall verifies that the entity is appropriately registered (for example, listed in the FCC Robocall Mitigation Database) and applies comparable due diligence. UnlimCall ceases to accept traffic from partners that are uncooperative or that prove to be a persistent source of illegal traffic.

7. Real-Time Call Monitoring and Heuristic Analytics

UnlimCall actively monitors network traffic using heuristic, AI-assisted analysis to detect behavior consistent with network abuse or robocalling and to act on it in near real time. Components include:

- **Traffic-pattern and anomaly detection.** UnlimCall baselines each customer's normal calling profile and watches for deviations characteristic of abuse — for example, sudden spikes in short-duration calls, extreme call-failure or non-completion rates, abnormal calls-per-second, or rapid sequential dialing across many destinations. Deviations generate alerts for automated mitigation or NOC review.
- **Per-line concurrency enforcement.** Each line is limited to one concurrent call, enforced on the network. This structural cap constrains the blast radius of any single compromised or abusive account and is a meaningful barrier to mass auto-dialing from a single credential.
- **Reputation and threat intelligence.** UnlimCall maintains internal blocklists of numbers and SIP identifiers associated with abuse and incorporates Do-Not-Originate (DNO) data and third-party reputation signals. Calls matching known-bad indicators are blocked or escalated, and the blocklist is updated as new intelligence is received.
- **NOC oversight.** UnlimCall's Network Operations Center has real-time visibility into traffic and alerts and is empowered to intervene — throttling, filtering, or suspending a trunk — when traffic matches an abuse signature. Automated controls handle instantaneous decisions while human analysts confirm and act on flagged incidents.
- **Tuning and review.** UnlimCall tracks the outcomes of its mitigation actions and periodically reviews thresholds and rules to improve detection of illegal traffic while limiting impact on legitimate calling.

UnlimCall describes here only the categories of analytics it operates; it does not claim detection capabilities it has not deployed.

8. Inbound and Outbound Robocall Mitigation Practices

UnlimCall screens, scores, throttles, or blocks suspect traffic in both directions so that illegal or unwanted calls are stopped as early as possible.

Outbound Call Mitigation

- **Caller-ID authentication.** Every outbound call is checked for an authorized caller ID and signed with STIR/SHAKEN attestation where eligible (Section 5). Calls with unauthorized or invalid caller IDs are blocked at origination.
- **Pre-call and in-flight checks.** Outbound attempts are evaluated against the customer's profile and account standing. Traffic that exceeds safe thresholds can be rate-limited or held; suspect streams can be intercepted or shunted for inspection.
- **Do-Not-Call and consent.** Customers conducting telemarketing or informational campaigns must scrub against the National Do Not Call Registry and their internal DNC lists, and must obtain and retain any legally required prior express consent (for example, under the TCPA for autodialed or prerecorded calls to wireless numbers). UnlimCall may require evidence of consent before permitting high-risk campaigns and halts campaigns where compliance cannot be demonstrated.

- **AUP enforcement.** Where outbound traffic violates the AUP — for instance an illegal robocall campaign or spoofed-number scam — UnlimCall may instantly suspend the trunk without prior notice, investigate, and terminate for cause if the activity is confirmed or not promptly remedied.

Inbound Call Mitigation

- **STIR/SHAKEN verification.** Inbound calls carrying an Identity header are cryptographically verified; calls that fail verification or present an untrusted signature are treated as suspect and may be rejected or labeled for the called party.
- **Analytics and blocking.** Inbound traffic is checked against internal and external spam and DNO lists; calls from numbers known for abuse, or from invalid or unallocated numbers, are blocked or diverted. Suspicious calls may be challenged or sent to screening, and blocked events are logged.
- **Upstream controls.** UnlimCall does not accept inbound traffic from domestic providers that have failed to file the required robocall mitigation certification, verifies interconnect partners against the FCC database, and blocks or throttles a source that begins sending unlawful or anomalous traffic pending resolution.

Outbound controls keep UnlimCall customers from originating illegal robocalls; inbound controls prevent external bad actors from reaching UnlimCall customers or abusing the network as a transit point. Both operate in real time and are continually updated.

9. Traceback Cooperation and Enforcement

UnlimCall cooperates fully with industry traceback efforts and law enforcement and enforces firm consequences against offending customers and partners.

- **Industry Traceback Group (ITG).** UnlimCall responds to traceback requests from the FCC-designated traceback consortium and from enforcement authorities via its NOC within 24 hours, providing the originating account, call timestamps, and routing data needed to identify the source of an identified call. A designated traceback point of contact is maintained in UnlimCall's RMD filing.
- **Customer cooperation obligation.** Under the AUP, customers must respond to ITG and fraud-investigation requests via UnlimCall's NOC within 24 hours. Failure to do so results in immediate suspension.
- **Law-enforcement cooperation.** UnlimCall responds to lawful requests for information and works with the FCC Enforcement Bureau, the FTC, and other authorities on robocall matters, handling data in accordance with its privacy obligations and applicable law.
- **Internal enforcement.** Where monitoring or a traceback indicates that a customer is originating unlawful calls, UnlimCall may instantly suspend the trunk without prior notice, permanently terminate the account, and — as provided in the AUP — withhold any prepaid balance as an administrative penalty. UnlimCall may provide the customer's KYC details and Call Detail Records to the FCC, law enforcement, or upstream traceback

consortiums. Upstream partners that fail to control illegal traffic are blocked and, if uncooperative, disconnected and reported.

- **Public reporting channel.** Anyone who believes an UnlimCall customer is violating the AUP, or who is receiving unwanted calls from a number on the network, may report the call details (time, receiving number, and caller ID) to abuse@unlimcall.com for investigation.

10. Data Retention and Audit Logs

UnlimCall maintains records sufficient to support traceback, enforcement, and regulatory audit, handled consistently with its GDPR and data-residency commitments.

- **Call Detail Records (CDRs).** UnlimCall retains CDRs including timestamps, origin and destination numbers, SIP identifiers, duration, routing, STIR/SHAKEN attestation or verification result where applicable, and disposition (completed, blocked, labeled). For compliance and traceback purposes, CDRs are retained for a minimum of 180 days (six months), configurable to a longer period per account on request. This floor is set deliberately above the window needed for immediate traceback so that records remain available for FCC Enforcement Bureau, FTC, or state Attorney General inquiries, which frequently concern campaigns several months old.
- **Preservation beyond default.** Records associated with flagged traffic, traceback responses, enforcement actions, or any matter UnlimCall knows to be under investigation are preserved beyond the default retention period under a litigation/preservation hold, so that evidence remains available to support investigations and audits.
- **Mitigation and enforcement logs.** Blocking, labeling, throttling, suspension, and termination events are logged with the reason, triggering criteria, and time, and are correlated to the underlying CDRs so that the handling of any given call can be reconstructed.
- **KYC and compliance records.** Customer identity and vetting documentation, signed AUP acceptances, and notes from compliance reviews are retained for the duration of the customer relationship and a defined period thereafter, with access restricted to authorized compliance personnel.
- **Data residency and security.** EU customer data is processed and stored in UnlimCall's Frankfurt and London regions; voice traffic terminates in-region and, where call recording is enabled, recordings are stored in EU object storage and are not used to train models. SIP signaling is protected with TLS 1.2+ and media with SRTP by default. UnlimCall's payment handling is out of PCI scope by design, as it does not capture DTMF, and a Data Processing Addendum is available pre-onboarding. Right-to-be-forgotten requests are honored consistent with overriding legal-retention obligations.
- **Audit support.** Because it retains these records, UnlimCall can demonstrate its STIR/SHAKEN status, its vetting steps under 47 CFR § 64.6305(d)(2)(ii), and its traceback responsiveness if audited by the FCC or another regulator.

11. Customer Education and Obligations

Effective robocall mitigation is a shared responsibility. UnlimCall imposes clear obligations on its customers through the AUP and Master Service Agreement and communicates expectations at onboarding.

- **Lawful use.** Customers must use UnlimCall services only for lawful purposes and in compliance with all applicable telemarketing and consumer-protection laws, including the TCPA and the Telemarketing Sales Rule in the US and the equivalent local regimes in international markets.
- **No spoofing.** Customers may transmit calls only from numbers they legally own or are explicitly authorized to use, and may not falsify, alter, or obscure caller-ID (ANI) information. They must not attempt to circumvent UnlimCall's call-signing measures.
- **Consent and DNC.** Customers are solely responsible for obtaining any legally required prior express consent, scrubbing against the National Do Not Call Registry and their own DNC lists, and honoring opt-out requests immediately.
- **AI-generated and prerecorded voice.** In accordance with the FCC's Declaratory Ruling FCC 24-17 (CG Docket No. 23-362, released February 8, 2024), AI-generated and voice-cloned calls are legally classified as "artificial or prerecorded voice" calls under the TCPA. Customers deploying UnlimCall's AI Voice Agents or Voice Cloning must obtain and retain prior express written consent (PEWC) where required, provide the required identification and disclosure at the start of the call, and offer a compliant opt-out mechanism. UnlimCall monitors this area, including the related pending FCC rulemaking on AI-generated call disclosures, and updates customer obligations as the rules evolve.
- **Prohibited activity.** Customers may not use the network for illegal robocalling, telemarketing fraud (tech-support, IRS/tax, wangiri, vishing/phishing), harassment, or toll fraud / artificial inflation of traffic, as enumerated in the AUP.
- **Traceback cooperation.** Customers must respond to traceback and fraud inquiries via UnlimCall's NOC within 24 hours and, where they resell or sub-lease service, must vet their own end users and assist in tracing them.
- **Education at onboarding.** UnlimCall communicates these requirements at signup, points high-volume and high-risk customers to the relevant consent and DNC practices, and engages directly with customers whose traffic patterns warrant clarification before they escalate into violations.

By requiring compliance at the source — the customer — in addition to UnlimCall's network-level controls, the program creates multiple layers of protection against illegal robocalls.

12. Point of Contact

For inquiries regarding this Robocall Mitigation Plan or UnlimCall's robocall prevention practices, and for traceback correspondence, please contact:

Daniel Schwartz

Chief Compliance Officer

UnlimCall LLC

Compliance / Traceback: compliance@unlimcall.com

Phone: 646 893 6777

125 Park Avenue 25th Floor New York, NY 10017, United States

This document has been prepared by UnlimCall LLC for informational and regulatory purposes. For inquiries, contact compliance@unlimcall.com.