

Robocall Mitigation Program – **HuSa** (FRN: **0037510617**)

1) Company & Service Scope

HuSa (Bogotá, Colombia) provides a multi-tenant softphone service for business and individual customers. We originate calls for our end-users and hand off U.S.-bound traffic to upstream U.S. gateway providers (e.g., Voxbeam). HuSa does not operate facilities in the United States.

2) STIR/SHAKEN Status

HuSa has no STIR/SHAKEN implementation obligation and has not implemented STIR/SHAKEN on any portion of its network. Where available, call authentication is performed by our upstream U.S. gateway providers.

3) Know-Your-Customer (KYC) & Onboarding

Individuals: government ID match + selfie/liveness (or equivalent) and verified email/phone.

Businesses: legal registry extract, tax ID, authorized signatory, domain control (DNS/WHOIS), and intended use case.

Sanctions/PEP screening where applicable.

Contract with Acceptable Use Policy (AUP) prohibiting illegal robocalls, spoofing, and violations of TCPA/FTC/FCC and local laws.

Risk scoring before enabling international or U.S./CA termination.

4) Caller ID (CLI) & Numbering Policy

Only authorized CLIs are allowed: (a) DIDs assigned by HuSa; or (b) customer-owned numbers with Letter of Authorization (LOA) / verifiable proof of ownership.

Enforce E.164 formatting; block invalid, unallocated, or impossible CLIs; apply Do-Not-Originate (DNO) lists.

The softphone UI does not permitir editar libremente el “From/CLI”; se selecciona de un inventario verificado.

Any attempt to circumvent CLI policies leads to immediate suspension.

5) Network & App Security (Softphone/PBX/SBC)

Strong SIP credentials (≥ 16 chars), TLS/SRTP where available, IP ACLs, device binding, and token-based session control.

Fraud controls: per-user/day caps, concurrency limits, geo/destination whitelists, and 2-factor changes for routing/CLI.

Automatic fail2ban-style blocking and SIP rate limiting against brute force.

6) Traffic Analytics & Real-Time Mitigation

Continuous monitoring of ASR, ACD, short-duration spikes, attempts/min, destination mix, and failure codes.

Real-time throttling/blocking when thresholds indicate potential illegal robocalls or hacked accounts.

Manual review within 24 hours; corrective actions include number/route blocks, account suspension, and customer re-verification.

7) Complaints & Traceback Cooperation

HuSa responds within 24 hours to traceback requests from the Commission, law enforcement, and the industry traceback consortium, and cooperates fully to stop illegal robocallers.

Traceback/Abuse Contact: Javier Ramos Rojas, Compliance Officer – [email@dominio] – [+57...].

8) User Education & AUP Enforcement

Clear in-app messaging: “privacy” means masking personal numbers using authorized DID, not anonymity to evade law enforcement or spoof identities.

Customer must maintain consent/legality of campaigns; violations lead to immediate blocking and termination.

9) Recordkeeping

Retain KYC artifacts, LOAs, CDRs, provisioning and blocking logs for 12–24 months (or longer if required by law).

10) Ongoing Compliance

Quarterly review of thresholds/KYC; staff training; periodic audits.

Filing updates in the RMD within 10 days of any material change.