

The one-page case

Open Voice Shield is one SIP hop on the trunk you already run. Every call that passes through comes back with a fraud verdict and the evidence for it, a route alert if the vendor cheated, and the audio quality of each leg; the next call from a flagged number is blocked or diverted automatically. It replaces nothing you have, installs nothing, and costs about eleven cents for a three-minute call. This page is written to be forwarded.

THE PROBLEM

The exposure is per call

Two kinds of loss arrive one call at a time, and nothing in a typical voice stack hears either of them happen.

Calls your customers make. A scam or an unlawful telemarketing call carries statutory exposure per communication: under the Telephone Consumer Protection Act, \$500 to \$1,500 per illegal call, uncapped. A non-compliant campaign that runs for a day has already generated a year's worth of damages before anyone reviews it.

Calls you pay for. A vendor route that answers on ringback, or swaps the far end to a recording a minute in, bills minutes nobody spoke. Manual test calls do not see it because the fraud is timed to outlast them.

CDRs show where calls went and for how long. Caller ID attestation shows who was allowed to present a number. Neither shows what was said, which is where both losses are decided.

TCPA STATUTORY DAMAGES

**\$500-
\$1,500**

per illegal call, no
aggregate cap

VERDICT AVAILABLE

minutes

after hangup, per call

TO INSTALL

nothing

one SIP hop, IP-
authenticated

One hop, three things on every call

- ✓ **A verdict with evidence.** Probability, category, the entity the caller impersonated, numbered red flags tied to what was said, a TCPA compliance note, and a block, review or allow recommendation, with the stereo recording and speaker-labelled transcript behind it.
- ✓ **A route alert.** Early answer on ringback, measured after the 200 OK, and delayed playback, read from the callee channel, reported separately from the caller verdict so it reaches the carrier relationship, not the fraud desk.
- ✓ **Call quality per leg.** Estimated MOS, jitter and packet loss for the caller leg and the callee leg, from the same capture, so a degrading vendor shows on the far leg while your side stays clean.
- ✓ **Enforcement on the next call.** Automation rules block or divert a flagged number for the window you choose; alerts go by e-mail or to your Slack channel; a signed webhook carries every verdict to your own systems.
- ✓ **Evidence you can hand over.** A branded PDF report, an offline export bundle with recording, capture and SIP log, and a password-protected share link.
- ✓ **Operable by software.** Everything above is typed data on the API, and an AI agent can run the whole account through the MCP server, from signup to a test call through your route to the verdict.

How it differs from what you already run

By approach, not by vendor. Most of these are complementary; none of them hears the call.

APPROACH	WHAT IT SEES	WHAT IT CANNOT DO	OPEN VOICE SHIELD
CLI reputation, STIR/SHAKEN attestation	The number and its attestation, at signalling time.	Hear the conversation. A well-attested number can still run a scam.	Reads what was said and acts on the number's next call. Keep attestation; add the verdict.
Call analytics and QA platforms	Recordings your own systems made, scored for quality or sales outcomes.	Record on any trunk, judge fraud and compliance, check the route, enforce.	Makes the recording itself as a SIP hop, scores fraud and TCPA, grades the route and the audio, blocks or diverts.
CDR-based fraud management	Destinations, volumes, durations, patterns, after the fact.	Catch one call on its content; explain why a call was bad.	Catches a single scam call on the words, with the red flags as the reason.
Manual route testing	A few short test calls a day, by hand.	See delayed playback timed to outlast the test; test every route every hour.	Reads every sampled live call, and an agent can test every route on a schedule with typed results.
An SBC or firewall	Signalling and media at the edge, by rule.	Understand the call. Rules need someone to know the bad number first.	Produces the bad number, with evidence, for the rule to act on.
Approaches to voice fraud and compliance, and what each one sees.			

What it is not: not a B2BUA replacement, not an SBC, not a campaign dialler, and not a real-time interruption of the live call. Verdicts are produced after hangup; enforcement is the next call from that number.

PROOF, AND WHAT WE DO NOT CLAIM

Judge it on your own traffic

The [technical white paper \(/whitepaper\)](#) describes the threat model, the call path, every pipeline stage and the measurement method; latency and transcription error were measured on a scripted corpus, and the method, corpus and raw results are shared on request. The [63-second film \(/#film\)](#) and the six-minute tour show the real product on a real scam call. The [documentation \(/docs\)](#) is written for the engineer doing the work, with every value taken from the running system.

We publish no accuracy, precision or recall figure, because none has been computed against a labelled corpus of real calls. The verdict is an analyst's read with its evidence attached, not a legal finding, and the TCPA note is a reading of the conversation, not legal advice. Estimated MOS is an estimate from loss and jitter, never a measured opinion score.

The honest way to evaluate it is the one we designed for: route one call in ten through the hop for a week, read the verdicts against what your team already knew, and count the route alerts.

What is always true on every call

- Nothing is injected into the live audio; analysis runs after the BYE.
- The ingress fails closed: if we are unreachable, your switch takes its normal alternate route.
- Every call keeps its recording, capture and SIP ladder as evidence.
- Recordings live in storage we control, with real retention deletion, and every endpoint is scoped to one tenant and audited.
- Analysis can run entirely on our own servers, with no third-party AI involved.

WHO USES IT

Three teams, three jobs

Carrier and wholesale NOC

Sample live traffic through the hop and catch early-answer and delayed-playback FAS on vendor routes with the evidence to take to the vendor. Let an agent test every route every hour. [FAS detection \(/fas-detection\)](/fas-detection).

Contact centre and compliance

A TCPA note on every analyzed call minutes after hangup, alerts when a campaign crosses the line, and the transcript counsel asks for. [TCPA penalty prevention \(/tcpa-compliance\)](/tcpa-compliance).

CPaaS, CCaaS and UCaaS platforms

Put a fraud verdict and a quality score on every call your customers make, by API and webhook, with automation on the next call. [Built for agents \(/docs/agents\)](/docs/agents) and [the API \(/docs/api-reference\)](/docs/api-reference).

COMMERCIALS

What it costs

One formula: analyzed minutes at the plan rate, plus one analysis fee per call, prepaid. On the default plan a three-minute checked call is about **\$0.11**, with recording, transcription, analysis and evidence included. No seats, no monthly minimum on pay-as-you-go, and \$5 of credit at signup so the first calls need no card. Bundled plans trade a monthly fee for a lower rate. The [pricing page \(/pricing\)](/pricing) reads its figures from the live plans API.

NEXT STEP

Put one call through it

Whitelist an IP, point a trunk, place one test call: the first verdict lands the same afternoon. Or hand the whole setup to an agent.

© 2026 Open Voice Shield: powered by TelecomsXChange. All rights reserved.