

# **Eiktel - ROBOCALL MITIGATION PLAN**

## **UPDATED - FEBRUARY 2026**

### **PURPOSE AND SCOPE**

Eiktel is a small voice service provider that originates voice traffic to the public switched telephone network and maintains a robocall mitigation program consistent with 47 CFR § 64.6305, including STIR/SHAKEN caller ID authentication implemented pursuant to 47 CFR § 64.6301(a), and may update its filing and associated plan information within 10 business days when filing information changes.

### **PROVIDER ROLE**

Eiktel provides Hosted PBX service to end-user customers only. Calls are made by those end users using extensions/devices we provision and support. We process calls through our hosted PBX platform as part of delivering service.

### **STIR/SHAKEN STATUS**

Eiktel certifies that it has implemented STIR/SHAKEN caller ID authentication consistent with 47 CFR § 64.6301(a). Our voice network is entirely IP-based, and we sign calls that originate on our network using in-house signing systems and our own STI certificate.

Eiktel applies the appropriate attestation level (A/B/C) based on what it knows about the calling party and the calling party's right to use the calling telephone number(s) consistent with applicable FCC rules, orders, and guidance.

### **ROBOCALL MITIGATION MEASURES**

- Eiktel maintains a practical, small-business customer onboarding process focused on verifying legitimate end users and preventing misuse. At onboarding, we collect and verify basic business identity information and validate customer payment details. Many customers are installed on-site, and in many cases, we have an established relationship with the customer.
- Enhanced review is triggered when risk indicators are present, including high call volume, short-duration calling spikes, or marketing/dialing use cases.
- Our traffic is monitored using in-house applications on FreeSWITCH, including ASTPP and custom scripts. Since our network and traffic volumes are small and consistent, abnormal spikes or unusual calling behavior are easier to detect quickly.
- If we see suspicious or illegal activity, we can rate-limit, block, and/or suspend service while we investigate. If it's confirmed misuse, we terminate service.
- We do not accept traffic from upstream providers, resellers or partners. We only carry traffic associated with our own end-user customers.

### **TRACEBACK COOPERATION AND RESPONSE**

We have a designated point of contact and we commit to responding fully within 24 hours to traceback requests from the FCC, law enforcement, and the traceback consortium, and we will cooperate by providing relevant call records and supporting details as requested.