

Cyberlife

Robocall Mitigation Program Description

1. Company Overview

Cyberlife is a Voice Service Provider that originates and routes voice traffic over IP networks interconnected with the public switched telephone network (PSTN). Cyberlife maintains an active certification in the FCC Robocall Mitigation Database. All voice traffic originating on the Cyberlife network is governed by the policies and controls described in this program.

2. Governance and Responsible Party

Cyberlife has designated a Compliance Officer responsible for oversight of STIR/SHAKEN implementation, robocall mitigation policy enforcement, traceback response coordination, and maintaining accurate Robocall Mitigation Database filings. Contact information is updated within 10 business days of any change. Senior management periodically reviews compliance posture.

3. STIR/SHAKEN Implementation

Cyberlife has implemented the STIR/SHAKEN framework in the IP portions of its network. All outbound calls are signed in accordance with FCC requirements. Attestation levels (A, B, or C) are assigned based on customer vetting and caller ID authorization procedures. Certificate lifecycle management procedures are maintained to ensure renewal and validity.

4. Customer Vetting and KYC Controls

Cyberlife applies documented Know-Your-Customer procedures prior to activating outbound calling services. These include verification of business identity, validation of contact information, review of intended call use cases, and confirmation that customers are authorized to use presented caller IDs. Customers are contractually required to comply with federal and state telemarketing laws.

5. Traffic Monitoring and Analytics

Cyberlife utilizes automated monitoring tools and analytics to detect anomalous traffic patterns, including high call volume with low duration, burst traffic, and unusual patterns inconsistent with stated business purposes. Suspicious traffic may be suspended, investigated, blocked, or escalated.

6. Mitigation and Enforcement

If Cyberlife identifies traffic reasonably believed to be illegal robocalling or spoofing, the originating customer is notified, traffic may be suspended, and service may be terminated for violations. Cyberlife maintains a zero-tolerance policy for knowingly transmitting illegal robocalls.

7. Upstream and Interconnection Controls

Cyberlife verifies that upstream and downstream voice providers are listed in the FCC Robocall Mitigation Database and properly certified. Cyberlife does not knowingly accept traffic from non-compliant providers.

8. Traceback Cooperation

Cyberlife cooperates fully with the FCC, the Industry Traceback Consortium, and law enforcement agencies. Traceback requests are responded to within 24 hours.

9. Recordkeeping

Cyberlife maintains records related to customer onboarding, STIR/SHAKEN implementation, attestation procedures, traffic monitoring investigations, and traceback responses. Records are retained in accordance with internal compliance policies.

10. Ongoing Review

Cyberlife reviews and updates its Robocall Mitigation Program as needed to address evolving threats and regulatory updates. Robocall Mitigation Database certifications are updated within 10 business days of material changes.