

Robocall Mitigation Program

BrightArrow Technologies, Inc.

Updated February 2026

1. Provider Classification

BrightArrow Technologies, Inc. operates as an **Originating Voice Service Provider (OVSP)**.

BrightArrow originates SIP-based outbound voice traffic from its managed network infrastructure and delivers calls to the Public Switched Telephone Network (PSTN) via contracted upstream carriers using IP-authenticated SIP trunks.

BrightArrow is a non-facilities-based provider and does not operate PSTN switching facilities.

2. STIR/SHAKEN Implementation

BrightArrow originates IP-based voice traffic and relies on upstream carrier partners to implement STIR/SHAKEN authentication in the IP portions of the network.

BrightArrow does not independently operate an STI certificate and does not directly sign calls.

Outbound calls are authenticated and signed by upstream carrier partners in accordance with their policies. BrightArrow has been informed that B-level attestation is applied to applicable outbound traffic.

BrightArrow supports appropriate attestation by:

- Maintaining verified customer relationships
- Validating authorized outbound caller ID numbers
- Restricting unauthorized caller ID usage

Attestation assignment is performed by upstream carriers consistent with industry standards.

3. Nature of Service

BrightArrow provides automated and interactive notification services exclusively to verified institutional customers, primarily K-12 schools, school districts and authorized educational entities.

BrightArrow does not provide:

- Consumer dial-out services
- Anonymous SIP access
- Bulk traffic resale
- Open trunking access
- Third-party traffic aggregation

All outbound voice traffic originates from authenticated institutional customer accounts within BrightArrow's platform.

4. Customer Vetting and Onboarding Controls

BrightArrow implements institutional customer verification prior to activation, including:

- Verification of organizational identity
- Execution of service agreements prohibiting unlawful robocalling
- Validation of authorized outbound caller ID numbers
- Controlled provisioning of sending accounts

Access to outbound voice functionality is restricted to authenticated, authorized institutional users.

5. Caller ID Integrity Controls

BrightArrow enforces caller ID integrity through:

- Validation of outbound telephone numbers prior to activation
- Prevents caller ID modification by customers, thus preventing unapproved number usage

Outbound traffic is limited to validated numbers associated with verified institutional customers.

6. Traffic Monitoring and Network Controls

BrightArrow employs layered monitoring and technical controls designed to prevent abusive or anomalous traffic patterns, including:

- Calls-per-second (CPS) thresholds
- Channel concurrency limits
- SIP rate limiting at gateway level
- Dial plan routing restrictions
- Continuous Call Detail Record (CDR) monitoring
- Monitoring of Answer Seizure Ratio (ASR)

These controls are enforced within BrightArrow's SIP proxy and switching environments.

7. Abnormal Traffic Detection and Mitigation

If abnormal or suspicious traffic patterns are detected, BrightArrow may:

- Suspend outbound campaigns
- Investigate customer activity
- Contact the customer for clarification
- Terminate service if violations are confirmed

BrightArrow maintains real-time capability to disable outbound traffic.

8. Traceback Cooperation

BrightArrow cooperates with:

- Upstream carrier traceback requests
- Industry traceback consortium inquiries
- Regulatory authorities

Call Detail Records (CDRs) and SIP logs are retained consistent with regulatory and carrier requirements to support traceback investigations.

9. Record Retention

BrightArrow retains:

- Customer onboarding documentation
- Caller ID authorization records
- Call Detail Records

Records are maintained in accordance with applicable FCC and carrier obligations.