

Robocall Mitigation Plan

Provider Name

BLaST Intermediate Unit 17 (IU17)

FCC FRN

0012461901

Regulatory Contact

Tim Confer, Director of Technology

tconfer@iu17.org

570-323-8561 x [1057]

Business Model

IU17 provides voice services on a resale basis. All calls are routed through Sangoma SBC equipment and delivered to upstream carriers including Zito, ClearlyIP, Comcast, and Broadvoice. These carriers perform STIR/SHAKEN signing and provide additional monitoring and mitigation. IU17 does not operate as a facilities-based carrier.

Company Overview

IU17 delivers voice services only to a limited and well-defined customer base. Service is restricted to public school districts, government agencies, and a small number of established nonprofit organizations. We do not sell to the general public or to unknown retail businesses. Every customer relationship is contractual and tied to a known institution, which significantly reduces the risk of abuse.

Caller ID Authentication

IU17 does not directly sign calls with STIR/SHAKEN. All outbound traffic is delivered to upstream carriers that handle signing and attestation. Calls are signed at the highest level possible based on the relationship between IU17, the customer, and the assigned numbers. IU17 does not bypass these processes and ensures all traffic is passed through compliant carriers.

Customer Onboarding

New customers are limited to the institutions described above. Each is verified through established organizational contacts and service agreements. Numbers are assigned only to those customers, and outbound caller ID use is restricted to numbers assigned through IU17 or its upstream carriers. Spoofing or misrepresentation of caller ID is not permitted. Requests for departmental or masked caller ID use are only honored when they map to numbers legally assigned to the institution.

Traffic Monitoring

All outbound calls are routed through Sangoma SBC equipment, which enforces strict access controls. Only pre-authorized customer IP addresses are able to reach the SBC. Fraud detection rules, including SIPVicious scanning protections, are enabled to block suspicious SIP traffic. Certain trunks are capped at 24 simultaneous calls to prevent overuse or abuse.

Most traffic is subject to filtering and monitoring by upstream carriers before termination. These carriers provide real-time detection, reputation scoring, and robocall analytics. IU17 retains full call detail records for all calls and can investigate any customer endpoint immediately if suspicious traffic is reported.

Complaint Handling

Any complaints about suspected robocall traffic are directed to voiceservices@iu17.org, which is tied to our ticketing system. Reports are escalated directly to Tim Confer, Director of Technology, at tconfer@iu17.org. Complaints are acknowledged within one business day, investigated within two business days, and resolved as quickly as possible. Investigations use SBC call detail records along with upstream carrier data. If a violation is verified, IU17 will disable the customer endpoint or suspend service immediately.

Cooperation with Traceback

IU17 cooperates fully with the USTelecom Industry Traceback Group and with regulatory authorities. We promptly identify the source of calls on our network and provide information on upstream or downstream providers and the associated customer. Contractual terms do not restrict our ability to cooperate in traceback requests.

International and High-Risk Traffic

International calling is not enabled by default. It is only permitted when specifically requested by an authorized institutional contact. Even then, it is restricted to designated phone numbers, and the upstream carrier enforces the controls. This prevents broad exposure to international fraud and keeps outbound traffic narrowly limited to legitimate institutional needs.

Numbering and Caller ID Practices

All direct inward dial (DID) numbers are obtained through Zito, ClearlyIP, Comcast, or Broadvoice. Caller ID presentation is limited to numbers assigned to that customer. Unauthorized spoofing is not allowed.

Record Retention

IU17 retains call detail records for a minimum of twelve months. Additional records can be obtained from upstream carriers if needed. Records are stored securely and are available for traceback or investigative purposes.

Enforcement and Remediation

If suspicious or abusive activity is detected, IU17 has the authority to take immediate steps to stop it. This includes blocking destinations, rate limiting, disabling endpoints, or suspending service. Customers who engage in prohibited activity risk termination of service. All actions taken are documented and shared with upstream providers as appropriate.

Governance

This plan is maintained by the Director of Technology and is reviewed annually or whenever FCC requirements change. Updates are reflected in the FCC Robocall Mitigation Database and in the public version of this plan.

Certification

IU17 certifies that it has implemented the measures described in this plan, that it cooperates fully with traceback requests, and that it will not knowingly facilitate unlawful robocall traffic.



Tim Confer

Director of Technology

BLaST Intermediate Unit 17

9/3/2025