

BLUECALLING HUB, INC.

ROBOCALL MITIGATION PLAN

Effective Date: August 14, 2026

Bluecalling Hub, Inc. (“Bluecalling” or the “Company”) maintains the robocall mitigation program described in this Plan to prevent its network and services from being used to originate illegal calls.

Bluecalling is a domestic voice service provider serving residential and business end users through IP-based voice services and related access platforms. This Plan applies to calls originated through Bluecalling’s services.

1. Company and STIR/SHAKEN Status

Bluecalling is a domestic voice service provider directly serving residential and business end users. Its voice network is IP-based.

Bluecalling has obtained:

- **FCC Registration Number (FRN): 0038517629**
- **FCC Form 499 Filer ID: 838997**
- **Operating Company Number (OCN): 503M**

Bluecalling has filed a current FCC Form 499-A, which has been accepted.

Bluecalling is registered with the STIR/SHAKEN Policy Administrator and has obtained its own SPC token and STIR/SHAKEN digital certificate from an approved Certificate Authority.

Bluecalling has implemented the STIR/SHAKEN authentication framework across its IP-based voice network and authenticates the calls it originates using its own STIR/SHAKEN certificate in accordance with applicable FCC requirements.

Accordingly, Bluecalling certifies to **Complete STIR/SHAKEN Implementation** pursuant to 47 C.F.R. § 64.6305(d)(1)(i).

Bluecalling will maintain its STIR/SHAKEN registration, certificate, and authentication capabilities and will update its Robocall Mitigation Database filing within 10 business days of any change requiring an update under 47 C.F.R. § 64.6305(d)(5).

2. Know Your Customer and Service Controls

Consistent with 47 C.F.R. § 64.1200(n)(4), Bluecalling takes affirmative and effective measures designed to prevent new and renewing customers from using its services to originate illegal calls. The measures applied depend on the service and customer relationship.

For account-based residential and business voice services, including application-based and SIP/VoIP services, Bluecalling obtains and reviews applicable customer identification, contact, address, account, billing, and payment information.

Material inconsistencies, suspicious information, or unusual account activity may result in additional review, restriction, denial, suspension, or termination of service.

Bluecalling also provides certain prepaid access-number services using customer PINs. For transactions made directly through Bluecalling, the Company maintains available purchase and transaction information. Where such services are distributed through third-party retail channels, Bluecalling may not receive identifying information regarding the ultimate purchaser.

These services are subject to technical and usage controls, including a single concurrent-call limitation, usage limits, a maximum call duration of two hours, caller-ID controls, and Bluecalling's internal traffic monitoring.

3. Caller-ID Controls

Bluecalling prohibits unlawful caller-ID spoofing and does not permit customers to select arbitrary external caller-ID numbers.

For account-based voice services, caller ID is limited to numbers assigned, provisioned, ported, or otherwise authorized for the applicable customer account.

For access-number services, Bluecalling presents the calling-party number received with the inbound access call and does not permit the customer to substitute an arbitrary caller-ID number.

Attempts to use unauthorized caller-ID information may result in restriction, suspension, or termination of service.

4. Internal Robocall and Fraud Analytics

Bluecalling performs its robocall and fraud analytics internally and does not use a third-party call-analytics or fraud-monitoring vendor.

Bluecalling uses an internal rules-based monitoring process that evaluates available call-detail records, customer account activity, traffic volume and calling patterns, caller-ID activity, platform information, complaints, and traceback information.

Internal rules and thresholds are used to identify unusual traffic, calling patterns, or account activity requiring additional review. Traffic meeting applicable monitoring criteria is flagged for investigation.

Depending on the circumstances and results of the review, Bluecalling may apply calling or usage restrictions, rate limits, suspension, or termination of service.

Confirmed intentional illegal robocalling, unlawful caller-ID spoofing, or fraud may result in suspension or termination.

5. Do-Not-Originate Blocking

Bluecalling applies reasonable do-not-originate blocking measures as required by 47 C.F.R. § 64.1200(o).

Bluecalling maintains appropriate safeguards for emergency calls and public-safety communications.

6. Know Your Upstream Providers

Bluecalling uses third-party telecommunications providers for call transport. These providers do not perform Bluecalling's robocall mitigation or fraud analytics.

Bluecalling does not provide wholesale transit or intermediate carriage services for unrelated voice service providers.

Consistent with 47 C.F.R. § 64.1200(n)(5), Bluecalling takes reasonable and effective steps concerning originating or intermediate providers from which it directly receives traffic.

Where applicable, Bluecalling verifies the Robocall Mitigation Database status of directly connected providers and maintains available information concerning the provider's legal business identity, contact information, role in the call path, contractual relationship, and applicable FCC identifiers.

Bluecalling periodically reviews applicable provider information and investigates credible indications that a directly connected provider is associated with a high volume of illegal traffic. Bluecalling may restrict or terminate a relationship where appropriate.

7. FCC Notifications and Required Blocking

Upon receipt of a Notification of Suspected Illegal Traffic from the FCC Enforcement Bureau under 47 C.F.R. § 64.1200(n)(2), Bluecalling will promptly investigate the identified traffic and report the results of its investigation within the timeframe specified by the Enforcement Bureau.

Where Bluecalling is determined to be the originating provider for identified illegal traffic, Bluecalling will take the blocking, mitigation, certification, and reporting actions required by 47 C.F.R. § 64.1200(n)(2), including blocking identified and substantially similar traffic on an ongoing basis where required.

Where Bluecalling determines that the traffic is not illegal or that it was not the originating provider, Bluecalling will provide the explanation and information required by the applicable FCC rule.

Bluecalling will monitor applicable Enforcement Bureau Final Determination Orders published in **EB Docket No. 22-174** and will block and cease accepting traffic received directly from a provider subject to such an order as required by 47 C.F.R. § 64.1200(n)(3).

8. Prior Enforcement Actions

Within the previous two years, neither Bluecalling nor any entity with which Bluecalling shares common ownership, management, directors, or control has been the subject of a formal Commission, law-enforcement, or regulatory-agency action or investigation with accompanying findings of actual or suspected wrongdoing due to transmitting, encouraging, assisting, or

otherwise facilitating illegal robocalls or spoofing, or due to a deficient Robocall Mitigation Database certification or mitigation program description.

9. Traceback and Cooperation

Bluecalling commits to respond fully within 24 hours to traceback requests from the FCC, civil or criminal law enforcement, and the FCC-designated industry traceback consortium and to cooperate with those entities in investigating and stopping illegal callers using its services.

A traceback request or credible complaint identifying a Bluecalling customer or service will result in review and, where appropriate, investigation.

Bluecalling maintains reasonably available records sufficient to assist in identifying the responsible customer and call. Such records may include customer or account information, originating caller-ID number, destination number, date and time, call duration, and relevant endpoint, source-IP, session, access, or carrier information where available.

10. Investigation and Enforcement

Bluecalling prohibits use of its services for illegal robocalling, unlawful caller-ID spoofing, fraud, or other unlawful calling activity.

When Bluecalling identifies credible indications of unlawful or abusive traffic, it investigates the activity and may restrict calling capabilities, impose rate or usage limits, suspend service, or terminate the responsible account.

Bluecalling cooperates with FCC, law-enforcement, and industry traceback investigations concerning traffic originated through its services.