

# Raw Calls Inc Robocall Mitigation Program

---

Draft for FCC Robocall Mitigation Database registration | Prepared 15 September 2026 | Status: operational facts and provider classification must be verified before certification

Raw Calls Inc adopts this program to prevent its voice network and services from being used to originate, carry, or process illegal robocall traffic. The program applies to every call path and business relationship for which Raw Calls Inc acts as an originating voice service provider, gateway provider, or non-gateway intermediate provider, as applicable. The company will certify only controls that it has implemented, tested, documented, and continues to follow. Any role that the company does not perform must be removed from the version uploaded to the FCC.

## Governance and scope

The designated robocall mitigation officer [name, title, direct telephone number, email] owns this program, reviews escalations, maintains a monitored traceback channel, and has authority to suspend traffic. A backup officer [name and contact] covers absences and after-hours requests. Network operations, customer onboarding, and compliance staff carry out the controls described below. The officer reviews the program quarterly, after material changes to call routing or analytics, and after any significant complaint, traceback, or enforcement notice.

Before filing, Raw Calls Inc will map its actual call paths and identify which calls it originates on behalf of end users, which calls it receives directly from upstream providers, whether any foreign-originated calls enter the United States through its network, and which calls it merely transits. Raw Calls Inc will record its actual IP and non-IP network segments, STIR/SHAKEN signing and verification arrangements, any approved extension or exemption, and the certificate holder or signing vendor. Authentication status and any extension claimed in the portal must match this inventory.

## Customer admission and ongoing oversight

For services through which a new or renewing customer can originate calls, Raw Calls Inc uses affirmative, effective screening before activation or renewal. It verifies the customer's legal identity, principal place of business, authorized representative, beneficial ownership or responsible principals as appropriate, and the intended calling use case. It collects the customer's website or other business evidence, callback contact, expected call volume and destinations, source of telephone numbers, caller ID authorization, and any dialing or lead-generation partners. It evaluates complaints, traceback history, suspicious affiliations, and inconsistencies before granting access. Higher-risk customers receive enhanced review, smaller initial limits, and closer monitoring; an unverifiable or misleading customer is declined.

Customer terms prohibit illegal robocalls, unauthorized spoofing, misrepresentation of caller identity, and unlawful prerecorded or artificial-voice calls. They require cooperation with traceback and investigations and give Raw Calls Inc the ability to restrict or terminate service. For telemarketing customers, onboarding also collects the purpose and script of the campaign, dialing technology, lead and consent source, DNC practices, complaint handling, and records sufficient to substantiate claimed calling authority. Raw Calls Inc does not treat a consent document by itself as proof that a call is lawful. Staff periodically reassess active customers, including at renewal and whenever traffic or complaints diverge from the approved use case.

## Caller identity and authentication

Raw Calls Inc permits each customer to present only telephone numbers that it owns, has been assigned, or has been expressly authorized to use. It verifies number-right evidence and maps approved numbers to the

appropriate customer and trunks. It rejects invalid or unallocated caller IDs and presentation of numbers from a do-not-originate list maintained or received by the company, subject to proper emergency safeguards. Any changed caller ID, new campaign, or unexplained volume surge triggers review.

For IP calls subject to STIR/SHAKEN, Raw Calls Inc applies signing or verification in accordance with its actual role, network capability, and applicable FCC rules. It assigns an attestation level supported by the verified calling relationship and number rights; it does not claim full attestation solely because a customer selected a number. The officer reviews authentication failures and signing exceptions. The filing must specify whether implementation is full, partial, or none and accurately explain any uncovered traffic. [Identify the actual provider, certificates, affected trunks, and any applicable approved extension or exemption.]

### **Traffic monitoring and call analytics**

Raw Calls Inc monitors call-detail records, signaling and customer attribution, complaint and traceback data, and available analytics to identify patterns associated with illegal robocalls. Signals include unusual call volume or concurrency, rapid changes of originating numbers, very short calls, high failure rates, repeated calls to many destinations, geographic or time-of-day anomalies, invalid or unallocated numbers, deceptive caller ID, and spikes in complaints or traceback requests. Alerts are assessed against the customer's approved use case rather than treated as conclusive proof of illegality.

The systems used for these checks are [name in-house platform(s), rule engines, and third-party analytics vendor(s); specify which traffic they cover, their inputs, alert thresholds or risk scoring in general terms, and the actions taken]. If no formal analytics product is used, replace the preceding sentence with an accurate description of the manual and technical monitoring actually performed. Staff document the alert, customer, affected trunks and numbers, records reviewed, decision, and time of any restriction. The mitigation officer may throttle, block an affected campaign or number, suspend a customer, or terminate a relationship as warranted, while preserving evidence and appropriate emergency-call safeguards.

### **Know your upstream provider and traffic acceptance**

Before accepting a direct upstream connection, Raw Calls Inc identifies the provider's legal name, business address, FCC registration number and RMD entry when applicable, role in the call chain, responsible contact, source of traffic, and authorized trunk or IP addresses. It verifies that the provider appears in the RMD where required, is not removed or prohibited, and can respond to traceback; it records the check and reassesses the relationship at least quarterly and upon notice of a change or suspected illegal traffic. The company does not accept directly delivered traffic from an unlisted provider where FCC traffic-acceptance rules prohibit it.

Raw Calls Inc ties inbound calls to a named upstream provider and a specific trunk or account, rejects anonymous or unauthorized peers, and prevents a provider from using another provider's credentials. Where foreign-originated traffic is received, the company determines whether it acts as the U.S. gateway and applies any additional gateway authentication and mitigation duties before relying on a general intermediate-provider filing. The final submission will name the methods actually used to verify upstream providers and the frequency of RMD checks.

### **Traceback and incident response**

Raw Calls Inc commits to respond fully to traceback requests from the FCC, law enforcement, and the designated industry traceback consortium within 24 hours of receipt. A monitored address [traceback email] and phone [number], with an after-hours escalation route [method], direct requests to the mitigation officer and backup. Staff promptly identify the call, customer, originating number, upstream and downstream peers, timestamps and time zones, and available SIP and call-detail records; they provide the requested traceback information and

preserve relevant evidence. They cooperate with investigations and any applicable cease-and-desist notice, and take effective measures to stop suspected illegal traffic while the investigation proceeds.

When notified of suspected illegal traffic, staff open an incident, isolate the affected call path, investigate the caller and source, impose a proportionate restriction promptly, and verify that the traffic stopped. The officer records the rationale, remediation, communications, and follow-up. Repeat violations or a customer that cannot substantiate lawful calling authority lead to termination and further action as required. Requests, responses, and supporting records are retained under [verified retention policy] and are available for audit.

## **Public safety and filing maintenance**

No mitigation control may block a call placed to 911. Raw Calls Inc makes all reasonable efforts to avoid blocking calls from public safety answering points and government emergency numbers. Staff test and document the effect of blocking rules on these call categories before activation and after significant changes.

The mitigation officer reconciles this program and the portal submission with actual operations before the authorized company representative certifies. The filing states each applicable role, STIR/SHAKEN status, contact information, principals and affiliates, any relevant enforcement or investigation history required by the portal, and the 24-hour traceback commitment. Changes to information required in the RMD filing are updated within 10 business days; changes to CORES registration are updated within 10 business days. The company performs the required annual recertification by March 1 and pays applicable filing fees. Filing and recertification are not delegated without company review and approval.