

ROBOCALL MITIGATION PROGRAM DESCRIPTION

ACP SOLUTIONS LLC — FCC Robocall Mitigation Database Filing

Legal Entity	ACP SOLUTIONS LLC
Brand / DBA	Fast Connectivity; Fast ISP USA
FCC FRN	0038833489
Provider Model	Non-facilities-based voice service provider / reseller
Underlying Network	Third-party upstream voice carriers, including Skyetel and/or Telnyx, as applicable to the services and call paths in use
STIR/SHAKEN	ACP does not independently implement STIR/SHAKEN on its own network; applicable authentication is performed by the underlying upstream carrier (Skyetel and/or Telnyx, as applicable to the call path).

1. Program Purpose and Scope

ACP SOLUTIONS LLC maintains this written Robocall Mitigation Program to take reasonable steps designed to significantly reduce the origination, carrying, or processing of illegal robocall traffic through its voice services. The program applies to the SIP voice and telephone-number services that ACP provides or resells to legitimate business customers.

ACP's intended customer use cases include ordinary business communications such as customer support, service inquiries, appointment/service coordination, customer callbacks, and inbound customer calls. ACP does not intend its services to be used for illegal robocalling, unlawful spoofing, or other prohibited traffic.

2. Know-Your-Customer / Customer Vetting

ACP uses reasonable onboarding procedures to understand who its customers are and how they intend to use voice services. Before activation, ACP collects available business identity and contact information and reviews the customer's stated use case.

Where appropriate, ACP may review the customer's business website and other publicly available business information, confirm an authorized account contact, and request additional information when the proposed use case or traffic profile presents elevated risk.

Customers are required to use the service lawfully and comply with ACP's applicable terms, acceptable-use requirements, and upstream carrier requirements. ACP may decline, delay, restrict, or terminate service when customer information is insufficient or inconsistent with the proposed use case.

3. New and Renewing Customer Risk Review

ACP applies its customer-vetting procedures not only when a customer is first activated but also when a customer renews or materially changes its service, traffic profile, destinations, calling practices, or requested capacity.

Material changes may trigger a review of the customer's identity, stated business purpose, expected call volume, calling destinations, use of autodialing or prerecorded messages, and other relevant risk indicators.

Customers presenting unexplained high-risk or inconsistent activity may be subject to additional review, traffic restrictions, suspension, or termination.

4. Traffic Monitoring and Analytics

ACP reviews information reasonably available from its own systems and its upstream carriers to identify suspicious or potentially unlawful traffic. ACP's underlying upstream carriers include Skyetel and/or Telnyx, as applicable to the services and call paths in use, and ACP relies on the fraud, abuse, reputation, and traffic-monitoring analytics that its applicable upstream carrier makes available to it as part of its analytics system for identifying and blocking illegal traffic. ACP does not separately operate its own proprietary robocall analytics platform beyond the tools provided by its upstream carrier(s).

Available indicators may include sudden changes in outbound call volume, unusually high call attempts, repeated short-duration calls, abnormal answer/failure patterns, broad or unusual destination activity, customer complaints, carrier abuse notices, and traceback information.

Where an applicable upstream carrier provides fraud, abuse, reputation, analytics, or traffic-monitoring information, ACP uses that information as part of its investigation and mitigation process.

5. Investigation and Mitigation

When potentially unlawful or abusive traffic is identified, ACP investigates the relevant customer and traffic using information reasonably available to it.

ACP may compare observed activity with the customer's approved business use case, review relevant account and call information, contact the customer for clarification, and request supporting information.

When credible evidence of illegal robocalling, spoofing, or other prohibited use is identified, ACP may restrict traffic, suspend or terminate the account, block affected numbers or routes where technically available, and coordinate with the applicable upstream carrier.

ACP documents material investigations and mitigation actions to the extent reasonably necessary for compliance, carrier coordination, and future review.

6. Upstream Provider / Know-Your-Upstream Procedures

ACP uses established upstream voice carriers, including Skyetel and/or Telnyx, as applicable to the services and call paths in use, for underlying SIP connectivity and related carrier functions. ACP maintains information identifying the upstream carrier used for each applicable voice service and reviews carrier requirements applicable to those services.

ACP will cooperate with its applicable upstream carriers regarding abuse reports, traceback requests, suspicious traffic, caller-ID issues, and requests to investigate or stop illegal traffic.

ACP will not knowingly route traffic through an upstream provider that it knows is unsuitable for lawful voice service or that materially fails applicable carrier or regulatory requirements.

7. STIR/SHAKEN and Caller-ID Authentication

ACP SOLUTIONS LLC is a non-facilities-based voice service provider/reseller and does not independently implement the STIR/SHAKEN authentication framework on its own network infrastructure. Where applicable, STIR/SHAKEN authentication is performed by the underlying carrier, which may be Skyetel and/or Telnyx, depending on the call path.

ACP will cooperate with its applicable underlying carriers concerning caller-ID authentication, spoofing, traceback, and related robocall-mitigation matters. ACP will not claim that it independently implemented STIR/SHAKEN where the authentication function is performed by an upstream carrier.

8. Traceback Requests and Cooperation

ACP SOLUTIONS LLC commits to responding fully and within 24 hours to traceback requests from the Federal Communications Commission, law enforcement, and the industry traceback consortium, consistent with applicable FCC requirements.

Upon receiving a valid traceback request, ACP will identify the relevant customer/account and review available customer, telephone-number, SIP, call-detail, and upstream-carrier information; provide the requested information within the required timeframe; and cooperate in investigating and stopping illegal robocallers that use ACP's services.

9. Complaints, Abuse Reports, and Escalation

ACP reviews credible complaints and abuse reports concerning traffic associated with its customers. Reports may come from customers, upstream carriers, traceback entities, regulators, law enforcement, or other credible sources.

ACP records sufficient information to investigate the matter, assesses the traffic against the customer's stated use case, and takes proportionate action. Serious matters may be escalated to the upstream carrier or appropriate authority.

10. Blocking, Suspension, and Termination

ACP may take immediate or expedited action when traffic presents a credible risk of illegal robocalling, spoofing, fraud, or material abuse. Depending on the circumstances, actions may include blocking affected traffic or numbers, reducing capacity, suspending outbound service, suspending the account, or terminating the customer relationship.

ACP may also require remediation or additional verification before restoring service.

11. Recordkeeping and Program Administration

ACP maintains reasonable records relating to customer onboarding, material customer reviews, abuse reports, traceback requests, investigations, carrier communications, and significant mitigation actions.

The program is administered by the designated robocall-mitigation contact. ACP will periodically review its procedures and update them when material changes occur to its services, upstream-carrier arrangements, customer risk profile, or applicable FCC requirements.

12. Compliance Commitment

ACP SOLUTIONS LLC is committed to taking reasonable steps designed to significantly reduce illegal robocall traffic through its services, to knowing its customers and upstream providers as applicable, to cooperating with traceback and enforcement requests, and to investigating and mitigating suspected unlawful traffic.

ACP will maintain its RMD filing and robocall mitigation program consistently with its actual operations and applicable FCC requirements.

Filing entity: ACP SOLUTIONS LLC

Brand: Fast Connectivity / Fast ISP USA

FRN: 0038833489

Document purpose: Robocall Mitigation Program Description for FCC Robocall Mitigation Database filing

This document describes ACP SOLUTIONS LLC's intended and actual mitigation procedures and should be updated if the company's network architecture, upstream providers, or operational practices materially change.