

Alaska Communications Robocall Mitigation Plan

Pursuant to 47 C.F.R. § 64.6305, ACS of Alaska, LLC, ACS of Anchorage, LLC, ACS of Fairbanks, LLC, ACS of the Northland, LLC, ACS Long Distance, LLC, and Alaska Communications Internet, LLC (collectively known as “Alaska Communications” or “AC”) submit this report on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls, as of June 30, 2021. Alaska Communications declares that it qualifies for an extension of the implementation deadline pursuant to 47 CFR 64.6304(a) as a small voice service provider with fewer than 100,000 voice service lines and pursuant to 47CFR 64.6304(d) as the majority of its network relies on technology that cannot initiate, maintain, and terminate SIP calls.. Alaska Communications reserves the right to modify, add, delete, or otherwise alter any of the policies and procedures described in the plan at any time as it deems appropriate to reflect its business, its capabilities, and its needs.

COMPANY BACKGROUND

Alaska Communications (with its predecessors) has a 100-year history of delivering high-quality communications services to Alaska residents, businesses, government agencies, and institutions. Alaska Communications serves the Municipality of Anchorage as well as many remote rural areas throughout the state.

With the sole exception of the Municipality of Anchorage, all other Alaska Communications serving areas are rural for purposes of the Communications Act. The majority (52 of 70) of our markets are not on the interconnected power grid and road system, and 49 of our remote communities rely on satellite Time-Division Multiplexing (TDM) connectivity and are not Signaling System 7 (SS7) capable.

In our urban market, Anchorage, we have introduced Voice over IP (VoIP) capability to complement our legacy TDM network. Although we are constrained by lack of data connectivity between our remote communities, we are expanding VoIP services and replacement of the legacy TDM central offices with IP capable switches where practical.

Rural areas of Alaska considered to be “Bush” are those that are not accessible by the state’s road system, and that also typically lack access to a regional, interconnected power grid. Such communities are accessible only by plane, boat, barge, or snow machine, and communications facilities deployed there may require an independent power source.

Alaska Communications voice services are offered by these subsidiaries:

- **ACS of Alaska, LLC**, is the incumbent local exchange carrier (ILEC) for two study areas: (1) the City and Borough of Juneau (Juneau Study Area) and (2) Eielson Air Force Base and Fort Wainwright (Greatland Study Area).
- **ACS of Fairbanks, LLC**, also an ILEC, serves the City of Fairbanks and certain nearby areas (Fairbanks Study Area).
- **ACS of the Northland, LLC**, is the ILEC serving two study areas: (1) Sitka Borough and certain non-contiguous Bush areas, including part of Prince of Wales Island, Yakutat, Northway, Border City, and parts of the Aleutian Island chain (Sitka Bush Study Area) and (2) Kenai,

Soldotna, Kodiak, and areas outside Fairbanks, including Delta Junction, Nenana, and North Pole (Glacier State Study Area).

- **ACS of Anchorage, LLC**, is the ILEC serving the Anchorage area, including Joint Base Elmendorf-Richardson and certain small communities such as Girdwood and Hope (Anchorage Study Area).
- **ACS Long Distance, LLC** (“ACS-LD”), provides long-distance telecommunications services within Alaska, and between Alaska and other states, using a combination of its own facilities and those of other facilities-based carriers.
- **Alaska Communications Internet** offers local hosted PBX Voice over Internet Protocol (VoIP) and Session Initiated Protocol (SIP) Trunk services in Anchorage and five of our larger rural markets.

ROBOCALL MITIGATION PLAN (RMP)

The Alaska Communications Robocall Mitigation Plan (RMP) outlines the technology, policy, and practices implemented by Alaska Communications and subsidiary companies to address illegal robocalls. This document addresses both TDM and IP (SIP) portions of the communications network delivering services on behalf of:

Legal Name	OCN / CIC	Type
Alaska Communications Internet, LLC	085J	IP-enabled Service Provider
ACS Long Distance, LLC	5353	Interexchange Carrier
ACS of Alaska, LLC	3022	Local Exchange Carrier
ACS of the Northland, LLC	3030	Local Exchange Carrier
ACS of Fairbanks, LLC	3008	Local Exchange Carrier
ACS of Anchorage, LEC	3000	Local Exchange Carrier

OBJECTIVE

Alaska Communications’ RMP Policy will prevent the origination of illegal robocalls on our voice network and assist with tracing and stopping illegal robocalls originating on other service providers. This is achieved through:

- **Knowing our subscriber customers.** We will continue to verify our customers’ business license status and sell subscriber lines only to entities physically located in our local exchange service area.
- **Preventing CLID “spoofing.”** We will screen end subscriber lines to prevent the transmission of un-owned directory numbers on subscriber lines through Calling Line ID (CLID) screening and strict policy enforcement.
- **Rapid response to traceback requests.** ACS commits to respond fully, within 24 hours, to all traceback requests from the FCC, law enforcement, and the industry traceback consortium and to cooperate with such entities in investigating and stopping illegal robocallers using its service.
- **Suspending bad actors.** Our contract language and acceptable use policy allows for immediate suspension of accounts that originate illegal robocalls. Alaska Communications will investigate Federal Communications Commission (FCC) notifications of suspected robocalls, reply to the FCC in writing, and suspend services to originators of illegal robocall traffic.

- **Validate wholesale customers.** We will verify that all wholesale voice customers are registered in the appropriate FCC database.

KNOW THE END SUBSCRIBER

Alaska Communications companies sell end user business and residential voice services only to those located within the state of Alaska. We verify that each new subscriber account is a valid business, government, or consumer through the existing sales process. For both business and residential customers, we run an identity verification process which cross-references several information sources to positively identify the subscriber prior to service activation. Business customers must also have a valid Alaska business license. We do not offer voice services outside of this process control.

PREVENT CLID SPOOFING

Alaska Communications permits only the transmittal of customer assigned directory numbers (DNs) as the Calling Line ID (CLID) for calls originating on the Alaska Communications network.

For traditional POTS and VoIP subscriber lines, the CLID is assigned during the installation process and is either the DN assigned to the line or another DN on the same customer account.

For VoIP SIP and ISDN PRI subscriber trunks, the CLID may be signaled by the customers communication system (PBX). All numbers signaled by the customer's PBX are validated against the DID numbers assigned to the trunk on which the call is received by the Alaska Communications Central Office (CO) Equipment. If the customer signaled CLID does not match a DN assigned to the trunk, the call will be blocked or the customer's primary DN will be substituted (depends on CO equipment). If a customer wishes to transmit a DN as their CLID that is not assigned to their account, they must present proof of assignment with another carrier of the DN. In this case the CLID of the trunk will be statically assigned to this DN for all outbound calls on that trunk group and all other signaling from the customer PBX will be ignored by CO equipment.

RAPID RESPONSE TO TRACEBACK REQUESTS

Law enforcement and USTelecom Traceback Consortium requests are handled 24x7 by the Alaska Communications Integrated Network Management Center (INMC) . Service objectives are less than one business day. The Alaska Communications INMC is reachable at 907 564 1642 or inmc@acsalaska.com.

SUSPEND BAD ACTORS

Both wholesale (carrier) and subscriber contract language permit the suspension of services on discovery of robocall policy violation. Alaska Communications will validate all wholesale (carrier) voice termination customers are listed in the FCC database prior initial provision of services.

Upon written notification from the FCC's Enforcement Bureau, Alaska Communications will investigate the suspected traffic and respond to the Enforcement Bureau within 5 business days notifying them of our findings and any mitigation steps taken. Enforcement Bureau notifications may be emailed to acslegal@acsalaska.com.

VALIDATE WHOLESALE CUSTOMERS

New wholesale (service provider) voice customers will be validated against the Robocall Mitigation Database prior to service activation. Alaska Communications will only provide network termination services to wholesale customers listed in the FCC Robocall Mitigation Database as of September 28, 2021.

STIR/SHAKEN IMPLEMENTATION

The Alaska Communications voice network remains primarily time division multiplexing (TDM). As a result STIR/SHAKEN is not applicable to most traffic originating on the Alaska Communications network. Currently all local carrier interconnection is TDM for both CLEC and wireless carriers. All interexchange carrier trunks to Alaska Communications end office switches are likewise TDM.

The sole exception to TDM is for Alaska Communications Long Distance interstate calls. A portion of these calls are completed by our affiliate Long Distance interstate vendor EssexTel. These calls are converted to SIP and signed by EssexTel prior to completion.



TRACEBACK REQUEST CHECKLIST

USTELECOM TRACEBACK OR LAW ENFORCEMENT AGENCIES

- _____ 1. Disclosure request made on USTelecom Traceback Law Enforcement Agency (LEA) letterhead – attach the written request to this checklist. (received via email).
- _____ 2. Suspected illegal robocall detail shown on request.
- _____ 3. Type of information requested was identified.
- _____ 4. INMC did not release requested information until written LEA request received that complied with above requirements.
- _____ 5. Record INMCINMC time spent in complying with request:
_____ Minutes _____ Hours
- _____ 6. **Information provided to law enforcement**
_____ Subscriber information / telephone number / address per request
_____ Originating Trunk Group, Carrier and Call Trace Record (SAS Trace)
- _____ 7. Send a hard copy of the following to the Legal Technician in the ACS Legal Department (MS 65) the next business day:
- (a) the completed INMC Checklist
 - (b) the written request form
 - (c) the data released to the law enforcement agency

Signature of INMC Technician

DATE

Printed Name of INMC Technician



FCC ENFORCEMENT BUREAU – ILLEGAL ROBOCALL REPORT

INVESTIGATION CHECKLIST

- _____ 1. Disclosure request made FCC Enforcement Bureau letterhead – attach the written request to this checklist. (received via email)
- _____ 2. Suspected illegal robocall detail shown on request.
- _____ 3. Network Switch Engineering time to investigate suspected illegal robocalls.
_____ Minutes _____ Hours
- _____ 4. Investigation Results
_____ Traffic originated on subscriber lines of account # _____
Account Name _____
_____ Suspect traffic originated on wholesale customer network
Wholesale Customer _____
- _____ 5. **Information provided to Legal**
_____ Subscriber information / telephone number / address per request
_____ Originating Trunk Group, Carrier and Call Trace Record (SAS Trace)
- _____ 6. Send a hard copy of the following to the Legal Technician in the ACS Legal Department (MS 65) the next business day:
(a) the completed Checklist
(b) three trace call examples

Signature and Printed Name

DATE

TRACEBACK PROCESS STEPS

- 1) INMC receives a request for traceback from USTelecom Traceback consortium via email.
- 2) INMC retrieves call detail from SAS server showing originating trunk group.
- 3) INMC determines whether this is a tandem (from another carrier) or AC-end customer call.
- 4) INMC provides this information to USTelecom.
- 5) INMC completes form, attaches traces, and forwards to legal department.

FCC ENFORCEMENT BUREAU STEPS

- 1) Regulatory receives notice of violation.
- 2) Regulatory forwards details to Tier 1 to open a ticket for investigation and assigns ticket to Switch Engineering.
- 3) Switch Engineering investigates in < 1 business day and provides results to regulatory / legal team (meeting).
- 4) Legal team determines whether this is illegal traffic based upon business type.
- 5) If appropriate, Legal team directs Service Delivery to write suspend orders.
- 6) Legal team responds to FCC notice.