

Robocall Mitigation Plan Compliance with TRACED Act

Date	Company	OCN Numbers	Change Summary
May 3, 2023	First Communications, LLC (FirstComm)	Primary: 4604, 4852, 528A, 5917, 9682 Resale: 8315, 4199, 8195	Initial Version
October 25, 2024	First Communications, LLC (FirstComm)	Primary: 4604, 4852, 528A, 5917, 9682 Resale: 8315, 4199, 8195	Revised Version (Section I, last paragraph)

Objective: Establish and follow a policy that is compliant with the TRACED Act

I. Overview

The FCC requires that all providers certify in the Robocall Mitigation Database their status for compliance with STIR/SHAKEN. FirstComm has previously certified since June 21, 2022 that it is fully STIR/SHAKEN compliant as legally required. Further, the FCC now requires that fully compliant STIR/SHAKEN providers implement and certify the implementation of a Robocall Mitigation Plan in furtherance of industry efforts to prevent and detect illegal traffic from originating and/or transiting their networks.

The FCC requires providers like FirstComm to develop a Robocall Mitigation Plan that:

- details the reasonable steps taken to avoid originating illegal robocalls including know your customer and know your upstream provider processes;
- demonstrates a commitment to respond to traceback requests and to cooperate with investigating and stopping illegal robocalls; and
- is filed in the Robocall Mitigation Database to certify full implementation of STIR/SHAKEN and the institution of a Robocall Mitigation Plan.

This Robocall Mitigation Plan is submitted on behalf of FirstComm, a competitive local exchange carrier and VOIP provider that delivers technology solutions nationally. All calls that originate or transit FirstComm's network are subject to this Robocall Mitigation Policy.

FirstComm is a mid-size voice service provider with both TDM and SIP services in its network serving retail and wholesale customers as well as a reseller of voice services. FirstComm's parent holding company is Summit Data Services, Inc., and its controlling principal is Joseph R. Morris. FirstComm has partnered with Neustar Information Services, Inc., a trusted third-party call solutions provider, to implement STIR/SHAKEN within its network and has been fully STIR/SHAKEN compliant since certifying such compliance with the FCC in its Robocall Mitigation Database on June 21, 2022.

II. General Prohibition Against Illegal Robocalling

FirstComm end user services are subject to restrictions contained in FirstComm's retail and wholesale contracts. All FirstComm direct end user Service Agreements and Service Orders include the requirement that service is provided pursuant to the FirstComm terms of service including FirstComm's website Terms and Conditions of Business Use requirements (collectively, "T&Cs"). FirstComm's existing T&Cs specifically prohibit robocalling and activities normally associated with robocalling including, but not limited to:

- violating any applicable local, state, or federal laws, court or administrative orders or regulations while using FirstComm services and transmitting any communication that
 - would violate any laws, court or administrative orders, or regulations;
- generating robocalls, spam, junk faxes or unsolicited commercial or bulk calls, messages, prerecorded messaging, email or transmissions (or activities that facilitate or have the effect of facilitating the dissemination of such calls, messages, email or transmissions);
- using FirstComm services to engage in, or in connection with, fraudulent activities or abusive purposes;
- engaging in activity that constitutes high volume or excessive use and/or exceeds permitted access to, or parameters of, the FirstComm service including call duration requirements, incomplete call ratios, calls per second restrictions and typical call usage patterns;
- accessing, altering, circumventing or interfering with facilities and/or information by rearranging, tampering, spoofing or making an unauthorized connection with any equipment, facilities or system through any fraudulent means;
- using server devices or host computer applications that are broadcast to multiple servers or recipients such that they could enable bots or similar routines such as auto-responders or cancel-bots;
- interfering with the ability to fairly allocate capacity among users or otherwise degrading service quality for others;
- impersonating another person or entity with fraudulent or malicious intent or for any purpose in violation of law or regulation; and
- using any unlimited services or plans for outside conferencing, call forwarding, monitoring or transcription services, messenger, messaging, data transmissions, transmission of broadcasts, transmission of recorded material, auto, constant or iterative dialing, other connections that do not consist of substantially uninterrupted live dialog between individuals, or any other activity that would be inconsistent with normal and reasonable small business usage.

Through FirstComm's T&Cs, all direct end user customers acknowledge and agree that FirstComm may take action up to and including modification, denial, suspension, blocking, blacklisting or termination of service, with or without notice, for violation of these use restrictions.

Likewise, the FirstComm Wholesale Services Agreement (WSA) executed by each wholesale customer enables FirstComm to terminate the WSA and/or terminate, suspend or disconnect any service at any time upon any use of FirstComm services for unlawful, unauthorized or fraudulent purposes or in any unlawful or materially abnormal manner including in violation of the WSA authorized use policy that includes restrictions on short duration call traffic and excessive incomplete call ratios. The WSA requires FirstComm wholesalers to contractually bind their own end users to terms and conditions similar to the FirstComm retail T&Cs including those detailed above that prohibit robocalling and activities normally associated with robocalling. In addition, wholesalers agree to identify FirstComm as a third-party beneficiary of all such end user contractual terms with rights of enforcement directly against the wholesaler's end user.

III. Know Your Customer

FirstComm uses the mitigation technique of “Know Your Customer” as one process designed to prevent new and renewing customers from using FirstComm service to originate illegal robocalls. FirstComm is a mid-size, long-established provider that maintains a close relationship with its customers. Many FirstComm direct end users are small businesses without enough call paths to generate the high volume of traffic associated with robocalling.

FirstComm vets business customers by asking questions regarding personally identifiable information for additional security on each such customer account before activating service or making material changes to existing services. FirstComm has a screening process for new customers, particularly those requesting service at or above large volume calling capability levels:

- FirstComm does not deploy large volume calling capability as a residential service or at a residential location;
- All businesses requesting FirstComm service must provide a federal tax ID and verification as to the nature of the business;
- FirstComm vets customers by performing credit checks including Dunn & Bradstreet reporting on select customers and researching corporate names as needed with applicable state databases;
- FirstComm verifies addresses to look for overlapping/multiple deployed voice path subscriptions; and
- A FirstComm representative may visit business locations as part of sales, provisioning or training processes which will confirm the number of users at the location is appropriate for the volume of calling.

With respect to FirstComm wholesale customers, FirstComm does not provide service to applicable providers that are not compliant with FCC robocall requirements, and thus, are not certified in the FCC Robocall Mitigation Database to the extent required. Further, FirstComm provided written notice on March 27, 2023 to its existing wholesale customers regarding new FCC requirements to recertify in the Robocall Mitigation Database and adhere to additional obligations regarding Robocall Mitigation Plans and call authentication per STIR/SHAKEN protocols. Such wholesalers are subject to the same “Know Your Customer” screening processes as direct end user customers.

IV. Know Your Upstream Provider

FirstComm does not accept calls from any provider that is not effectively registered with the Robocall Mitigation Database as required by the FCC and applicable law. FirstComm has carrier contracts in place with its upstream providers to ensure it is not, directly or indirectly, facilitating or handling illegal robocall traffic. Such carrier agreements require the provider’s compliance with applicable laws including cooperation with traceback requests and robocall mitigation efforts. FirstComm vets all upstream providers in conjunction with its vendor setup processes including establishing federal tax ID, address/location and contact information. FirstComm will block all calls that it reasonably expects are transiting its network to pass illegal robocall traffic.

V. Network Monitoring

FirstComm's Network Team prepares analytics reports that will identify patterns consistent with illegal robocalling. Further, FirstComm has customer call detail records available to it for review with respect to significant deviations from typical call volumes for making determinations regarding the legitimacy of any such call volumes. For FirstComm wholesale traffic customers on its Sonus platform, FirstComm has implemented automatic call rejection for all calls that fail STIR/SHAKEN verification. In addition, FirstComm is reviewing such automatic call rejection processes for application in connection with its efforts at transitioning to a SIP network provider.

With respect to fraud detection generally, FirstComm uses a robust, industry-leading call analytics system provided by its third-party trusted vendor, in combination with FirstComm's 24x7x365 Network Operations Center team (NOC), to identify and block certain fraudulent call traffic. Equinix's software Protector service affords real-time monitoring of toll traffic on FirstComm's network and will flag call patterns indicative of fraud, including alerts for high fraud territories, excessive long duration or incomplete calling and call counts. When FirstComm's real-time Protector monitoring system identifies suspicious calls or calling patterns, an automatic email triggers both to FirstComm's fraud team indicating that established call thresholds have been violated and to the Zendesk ticketing system used by FirstComm that autogenerates a ticket with specific details for NOC technicians to assess for toll fraud.

In conjunction with its Network Team analytics, FirstComm seeks to identify any customer that is using the network to originate, route or terminate suspicious calls. These internal investigations can include verifying that the originating customer is authorized to use the caller number, suspending the customer's ability to originate or terminate calls on the FirstComm network and/or initiating a traceback investigation. When a customer's service is disabled due to suspicious calls or calling patterns, including illegal robocalling, FirstComm will not restore service at a customer's request without escalation for Vice President level review and approval which generally includes further consultation with Network Operations and Legal/Regulatory regarding call legitimacy.

If FirstComm receives reports of potentially illegal robocalling from an outside source such as a customer, peer carriers or traceback requests (discussed below), the FirstComm NOC will expeditiously initiate an investigation per the same investigatory approach.

VI. Traceback Efforts and Cooperation

FirstComm initiates traceback investigations with The Industry Traceback Group (ITG) as legally required with respect to its network traffic. Further, FirstComm actively cooperates with the traceback community including the FCC, law enforcement and ITG to investigate and stop illegal robocalls. A traceback investigation is the process of determining the origin of a call, typically starting with the receiving party and terminating service provider and tracing backwards through the path to the origin of the call. FirstComm has a Network Team that spearheads robocall mitigation efforts and a 24x7x365 NOC that conducts traceback request investigations. FirstComm will continue to dedicate sufficient resources to provide prompt and complete responses to traceback requests within the FCC required timeframes including within twenty-four hours for applicable requests.

VII. Enforcement

If, after appropriate investigation, FirstComm determines that illegal robocalls are likely originating or transiting its network, FirstComm stems the flow of such calls by warning the offending customer to discontinue such traffic and/or by terminating the service supporting such unlawful calling in accordance with applicable law, FirstComm legal terms and requirements and FirstComm policy. FirstComm will block all calls that it reasonably expects are transiting its network to pass illegal robocall traffic.

FirstComm Legal/Regulatory personnel routinely monitor efforts of the FCC and FTC regarding robocall mitigation efforts, identification of industry trends, provision of educational materials and other related information and alerts. FirstComm consults with outside legal counsel as required in connection with its robocall mitigation efforts, policies and enforcement.