

COMTELUS INC.
Robocall Mitigation Plan

Company Name: ComTelus Inc.
Company Address 3422 Old Capitol Trail., Wilmington DE, 19808
Company Phone #: 866-506-0550

Contact Information

Compliance Team
Phone: 866-506-0550
Email: compliance@comtelus.net

Overview

In the Commission's recent release, *In the Matter of Call Authentication Trust Anchor, Sixth Report and Order and Further Notice of Proposed Rulemaking*, WC Docket No. 17-97 (rel. March 17, 2023) ("R&O") it is stated that all voice service providers ("VSPs") must file robocall mitigation plans ("RMPs") that, among other things, outline "reasonable steps" taken to avoid originating illegal robocalls.

In addition to the "reasonable steps," the FCC requires that a RMP include:

- "know your customer" procedures;
- "know your upstream provider";
- ownership information;
- a description of any traffic analytics system used to identify and block illegal traffic; and
- whether a third-party vendor is used and if so, the name of the vendor.

The FCC previously stated that a RMP is sufficient if the detailed practices in the plan can reasonably be expected to significantly reduce the origination of illegal robocalls and the VSP complies with the practices it describes in its filing.

Purpose

ComTelus is a small service provider dedicated to stopping illegal transmissions from traversing the network and monitoring the transmissions coming into its network.

As certified in the FCC's Robocall Mitigation Database, ComTelus has fully implemented STIR/SHAKEN. In compliance with the R&O, ComTelus submits this RMP and certification. ComTelus Inc. may modify, add, delete or otherwise alter any of the policies and procedures described in the plan at any time in order to respond to changes in its business, its capabilities and its needs.

ComTelus Inc. only provides interconnected and non-interconnected VOIP services. The status of its STIR/SHAKEN implementation is:

- ☒ My traffic is fully attested.
- ☐ My traffic is partially attested.
- ☐ None of my traffic is attested yet

ComTelus Inc. has implemented the following Robocall Mitigation Plan to address unlawful transmissions :

1. ComTelus Inc. has enforceable terms of use and/or acceptable use policies noted in its contracts. These policies define the circumstances by which the company will deny, suspend, or terminate service to a customer. Prior to commencing services for new customers, the company takes the following measures to weed out end users that could potentially generate illegal or unlawful transmissions.
2. ComTelus Inc. will provide verified law enforcement and regulatory agencies with the relevant non-proprietary information in response to reasonable and legitimate requests about suspected illegal transmissions and suspicious activities, and implement mandated Robocall Mitigation Plan procedures to the fullest extent possible with the goal of maximizing the mitigation of illegal or unlawful transmissions.

ComTelus Inc. Know Your Customer ("KYC")

New ComTelus subscribers must provide the following information:

- Customer's identity / Customer's legal name and associated DBA's
- Customer's right to use the originator number presented on transmissions
- Customer Service Address
- Any past complaints or enforcement actions filed against customer
- VOIP telecommunications activity

ComTelus Inc. requires Business Incorporation Documents and verifies they have a reputation as a valid business that abides by the law.

ComTelus Inc. is a small company, we have a small number of customers. We know our customers and clearly understand their use cases.

3. ComTelus Inc. has established methods and procedures for monitoring network metadata activity to detect and prevent fraudulent activity. ComTelus Inc. employs transmission authentication, transmission labeling, and transmission blocking tools and services to protect its networks and consumers from harmful communications. ComTelus also uses software to monitor its network's usage patterns to aid in detecting suspicious activity and has established methods and procedures in place to address issues as soon as they are identified.

4. If any pattern of questionable activity is detected, ComTelus Inc. will provide notice to and require its customer to investigate and resolve any concerns expeditiously. If ComTelus Inc. is not satisfied with the customer's resolution, and/or the issue persists, and/or the issue identified warrants an immediate halt to any and all potential activity, ComTelus Inc. may, at its sole discretion and without notice to the customer, suspend and/or terminate all services for the customer in question.

5. Know Your Upstream Providers

In accordance with the Commission's directive in *Advanced Methods to Target and Eliminate Unlawful Robocalls Call Authentication Trust Anchor, Seventh Report and Order In CG Docket 17-59 and WC Docket 17-97, Eighth Further Notice of Proposed Rulemaking In CG Docket 17-59, and Third Notice of Inquiry in CG Docket 17-59* (Rel. May 19, 2023) ¶¶ 49-51, ComTelus Inc. provides the following information concerning its vendors.

ComTelus Inc. has agreements with seven vendors and has received assurances in writing from their officials they have, and will continue to abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing services to ComTelus. ComTelus Inc. and its vendors have agreed to work together diligently to mitigate illegal robocalls, including cooperating fully when receiving traceback requests.

6. Acceptable Use Policy ("AUP")

ComTelus has enforceable terms of use and/or acceptable use policies noted in its contracts. These policies define the circumstances by which the company will deny, suspend, or terminate service to a customer. ComTelus maintains an AUP that subscribers must agree to before being permitted to use its software and services. Among other things, the AUP prohibits:

- using our service for any illegal purposes whatsoever;
- engaging in activity for which FCC or any equivalent national regulatory authority, has restricted or regulated in relation to proper use of the public telephony network or the Internet;
- using our service if ComTelus determines, at its sole discretion, that its provision for this customer is prohibited by applicable law or has become impractical or unfeasible for any legal or regulatory reason; and
- using our service to offer or otherwise make available to others fraudulent goods, services, schemes, or promotions, including make-money-fast schemes, Ponzi and pyramid schemes, phishing, pharming, harvesting or similar deceptive practices.
- the sending of outbound traffic via the PSTN with Caller IDs not owned by the customer or the customer's subscribers.

7. If ComTelus Inc. receives notice that the Customer's outbound transmissions through its platform are deemed to be unlawful, ComTelus has the right to disconnect the service immediately and without notice.
8. ComTelus Inc. has complied fully, to the best of its knowledge, with all conditions set forth in the FCC's 2020 Report and Order mandating the implementation of the

STIR/SHAKEN framework, as well as with the Commission's rules and policies more generally.

9. ComTelus Inc. works to detect transmission patterns consistent with illegal robocalls. If such a transmission is detected, we will identify the party that is using our network to originate those communications and will take appropriate action. Taking appropriate action may include, but is not limited to, initiating a traceback investigation, verifying that the originating subscriber owns or is authorized to use the Originator ID number, and suspending or terminating the party's ability to originate transmissions on our network.
10. If any pattern of questionable activity is detected, ComTelus will provide notice to and require its customer to investigate and resolve any concerns expeditiously. If ComTelus is not satisfied with the customer's resolution, and/or the issue persists, and/or the issue identified warrants an immediate halt to any and all potential activity, ComTelus may, at its sole discretion and without notice to the customer, suspend and/or terminate all services for the customer in question.

Investigate Suspicious Activity

11. When traffic analysis indicates the presence of likely unlawful or non-compliant communications, ComTelus Inc.'s risk prevention team is alerted, which follows the defined procedures on investigating such users.
12. The procedures established include but are not limited to:
 - checking recent and past transmission detail records and benchmark against expected trends;
 - checking recent and past account activity and purchases;
 - investigating if any system issue generates the strange behavior;
 - verifying that the transmission originating path is valid; and
 - contacting the subscriber to understand his or her particular use case and validate that the activity belongs to that subscriber.
13. ComTelus Inc. has designated a dedicated response team as a direct point of contact for addressing traceback requests. It will provide the ITG with the contact information and business hours for this team upon receipt of the first request from the ITG. See <https://www.ustelecom.org/the-industry-rollback-group-itg-for-providers/>. ComTelus Inc. will respond promptly to inquiries from the Industry Rollback Group (ITG).
14. ComTelus participates in any traceback and trace forward investigations. To allow for timely and comprehensive responses, ComTelus devotes sufficient resources to provide prompt and complete resources to traceback requests. ComTelus has designated a dedicated response team as a direct point of contact for addressing traceback requests. ComTelus will respond promptly to inquiries from the Industry Rollback Group (ITG). It will provide the ITG with the contact information and business hours for this team upon receipt of the first request from the ITG.

15. Requests from the ITG must be submitted in writing, via email to tracebacks@comtelus.net and include the following information:

- Specific rule, regulation, code, or statute of alleged offense or non-compliance
- Nature of the Suspected Violative Communications
- Transmission Origination Number
- Transmission Recipient Number
- Date and Time of the Transmission
- Medium of the Transmission

16. ComTelus Inc. will cooperate with state and federal regulators and law enforcement to prevent any and all illegal or unlawful transmissions. For more information, please visit <https://comtelus.net/legal/> Requests from must be submitted via ComTelus Inc.'s online form at <https://comtelus.net/legal/> and include the following information:

- Law Enforcement or Agency Name
- Address:Requestor's Name
- Requestor's Title
- Requestor's contact Phone Number
- Requestor's Contact E-mail
- Nature of the Suspected Violative Communications
- Transmission Origination Number
- Transmission Recipient Number
- Date and Time of the Transmission
- Medium of the Transmission

17. Blocking

ComTelus will promptly respond to Do Not Originate requests it receives from the ITG. ComTelus has mechanisms to block suspicious transmissions. If ComTelus's monitoring systems identify suspected transmission patterns that are confirmed with further investigation, ComTelus will take appropriate action which may include suspending or terminating the user's access to ComTelus's network. ComTelus will cooperate with investigative bodies (provide a single point of contact to address traceback requests from law enforcement including state attorneys general offices), to the FCC, and/or the ITG; as well as documenting requests and actions taken in response thereto.

18. Plan Updates

This plan and industry best practices must evolve in response to the dynamic nature of mitigating illegal robocalling. ComTelus Inc. will monitor industry best practices and continuously improve its internal processes to ensure this plan and its system adapt to this ever-changing issue.

In the event of any material change to this plan, ComTelus Inc. will republish it to employees, consultants and contractors and file such an update to the FCC Robocall Mitigation Database within ten (10) days of such update.

Certification of James Collins

I, James Collins, CEO of ComTelus, Inc. do hereby certify, under penalty of perjury, the following:

- (1) ComTelus Inc. has fully implemented STIR/SHAKEN in the IP portions of its network.
- (2) ComTelus Inc.'s Business name and primary address are as follows:

ComTelus Inc.
3422 Old Capitol Trail
Wilmington DE, 19808
- (3) ComTelus Inc. has no other business names in use.
- (4) ComTelus Inc. has not previously used any other business name.
- (5) The name, title, department, business address, telephone number, and email address of the individual responsible for addressing robocall-related issues are listed in the above robocall mitigation plan.
- (6) The following entity owns more than 10% of ComTelus: Downeaster Holdings Inc. It did not have any licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding.
- (7) ComTelus Inc.'s role in the transmission chain is that of a service provider with a STIR/SHAKEN implementation obligation serving end-users.
- (8) ComTelus Inc. has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (9) ComTelus Inc. is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- (10) ComTelus Inc.'s Operating Company Number is 493K.



James Collins