

VERSCOM LLC.

501 Silverside Street Suite
105 Wilmington DE 19809 USA
legal@verscom.com

Robocall Mitigation Plan

April 28, 2024

Pursuant to 47 C.F.R. § 64.6305, Verscom, LLC. (“VERSCOM”) submits this report on its plan to prevent and mitigate illegal robocalls, as of April 28, 2024. VERSCOM 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.

Verscom LLC (“VERSCOM”) takes seriously fraudulent/illegal robocalling and malicious spoofing (collectively, “fraudulent robocalls”) and is committed to taking the necessary steps to mitigate fraudulent robocall traffic from traversing its network, including fully cooperating with federal and state law enforcement and government agencies and other telecommunications industry members in our collective effort to mitigate fraudulent robocalls.

Accordingly, VERSCOM has implemented the following Robocall Mitigation Plan (“RMP” or “Plan”), which is intended to meet the list of affirmative obligations placed on gateway providers by the Federal Communications Commission (“FCC” or “Commission”), including: (1) implementing effective measures to avoid carrying or processing illegal robocall traffic; (2) responding fully and within 24 hours to all traceback requests from the Commission, civil and criminal law enforcement, or the Industry Traceback Group (“ITG”); and (3) cooperating with the Commission, civil and criminal law enforcement, and/or ITG in investigating and stopping illegal robocallers that use VERSCOM’s service to carry or process fraudulent robocalls. Below, VERSCOM elaborates on the policies and procedures it has in place to meet each of these obligations. These measures are in addition to the onward transmission of any call attestation information that is received by VERSCOM in our capacity as an intermediate gateway provider.

I. Measures to Avoid Carrying or Processing Illegal Robocall Traffic

Based in part on recommendations proposed by ITG, and in response to the obligations the Commission has placed on gateway providers with respect to calls with a U.S. number in the caller ID field, VERSCOM has implemented a multi-pronged approach to monitor and police against fraudulent robocall traffic profiles, stopping such traffic profiles from being processed and sent to the United States. Under this approach, VERSCOM has taken the following steps:

- Implemented technical measures to identify and prevent suspicious call traffic patterns from entering its network;
- Trained VERSCOM technical staff on VERSCOM’s policies to limit fraudulent robocalls on its U.S. terminating network and procedures for assisting investigators; and
- Implemented policies and procedures to ensure VERSCOM’s upstream provider customers are not using VERSCOM to carry or process a high volume of fraudulent robocall traffic.

VERSCOM LLC.

501 Silverside Street Suite
105 Wilmington DE 19809 USA
legal@verscom.com

Technical Measures:

VERSCOM has implemented a series of technical measures to stop fraudulent robocall traffic.

First, VERSCOM analyzes its high-volume U.S.-destined traffic to look for calls with suspicious characteristics and identify upstream carriers that are sending this traffic. Review and analysis consists of some or all of the following elements as necessary:

- Comparison of historical traffic patterns to the suspect traffic patterns from the customer in question
- Comparison of traffic patterns to other customer traffic
- Manual test calls placed to the calling number
- Evaluation of quality statistics on the traffic in question to determine if providers are rejecting an abnormal proportion of the traffic or if completion rates are substantially lower than normal.

VERSCOM blocks traffic because it is traffic of a short duration, which is consistent with the characteristics of fraudulent robocalls. VERSCOM also contacts the upstream provider customer associated with those calls and informs it that its traffic has been blocked based on meeting the above criteria.

Second, VERSCOM monitors traffic that enters its domestic network from customers in foreign countries to ensure such traffic is not coming from a 1+ U.S.-originating number, is not an illegal robocall or number previously identified by U.S. authorities, including on a Do-Not-Originate (“DNO”) list, and does not have a pattern as described above. If U.S.-bound traffic originating from outside the United States meets any of these characteristics, that traffic is labeled as potentially malicious and/or fraudulent robocall traffic and is blocked. VERSCOM also contacts the customer associated with these calls and provides it with the notice detailed above.

Third, VERSCOM blocks suspicious traffic identified by ITG or United States authorities.

Fourth, VERSCOM maintains an internal Network Operation Center team that coordinates anti-fraud tasks with the Customer Service and Traffic Management Departments. The Network Operation Center functions 24 hours a day, 7 days a week and manages the search and detection of fraudulent traffic as well as escalation and notifications when such traffic is identified.

Fifth, VERSCOM only transmits calls originating from foreign countries into the foreign countries. It does not knowingly transmit calls originating from within the United States or to United States, and thus does not have any policies in place for monitoring telephone calls that originate from carriers in the United States.

Staff Education:

VERSCOM educates its personnel on how to identify fraudulent robocall traffic and the possible ways such traffic could enter VERSCOM’s network. VERSCOM management meets with VERSCOM personnel to instruct them on how to identify fraudulent robocall traffic that meets the criteria identified above. VERSCOM makes clear to its staff that it does not tolerate fraudulent robocall traffic on its network and that such traffic must be immediately blocked once identified. These policies are outlined in a guidance document that is distributed to each

VERSCOM LLC.

501 Silverside Street Suite
105 Wilmington DE 19809 USA
legal@verscom.com

staff member, and each staff member must agree to abide by these policies via a signed acknowledgement.

Verification of and Instructions to Upstream Carrier Customers:

In accordance with the FCC's new "know-your-upstream provider" requirement (3 See 47 C.F.R. § 64.1200(n)(4)) VERSCOM has implemented policies and procedures to ensure the upstream carrier customers whose traffic VERSCOM carries are legitimate voice service providers and/or intermediate providers and that such upstream carrier customers do not use VERSCOM to process a high volume of fraudulent robocall traffic.

First, VERSCOM follows procedures for ensuring it knows the identities of the upstream carrier customers from which it accepts traffic. VERSCOM vets the identity of its upstream carrier customers as part of the service initiation process, requiring these customers to provide VERSCOM with the customer's legal business name, tax or corporate registration number (if applicable), country of incorporation, business address, and contact information. VERSCOM also requires the customer to have a bank account in the same country of its incorporation. All of this information allows VERSCOM to identify any record of the customer across VERSCOM's and its affiliates services and may also be provided to third party agencies to determine the credit and/or fraud risk associated with the upstream carrier customer. VERSCOM can also use the customer's current contact information to confirm that the upstream carrier customer is registered in the Robocall Mitigation Database. If VERSCOM cannot validate the customer based on the initial information provided, VERSCOM may require additional information to validate the upstream carrier customer. VERSCOM will terminate or suspend service to upstream carrier customers with a history of non-compliance with its contractual obligations, including provisions relating to acceptable use of the service.

Second, any upstream carrier customer that contracts with VERSCOM is prohibited from abusive, fraudulent, or unlawful use of VERSCOM's services. If a customer is using VERSCOM's network for abusive, fraudulent, or unlawful purposes –including, but not limited to, transmitting fraudulent robocalls –VERSCOM's service agreement with the customer permits VERSCOM to terminate service to the customer. If an upstream carrier customer that has been terminated attempts to contract with a VERSCOM affiliate, the information gathered by VERSCOM will allow it to identify the upstream carrier customer as having been previously terminated.

Third, VERSCOM has implemented a process to ensure it contacts its upstream carrier customers after suspicious traffic is identified and blocked to inform them that their U.S. terminating traffic has been blocked until further notice because it violates applicable U.S. federal and state antirobocalling and consumer protection laws. Additionally, where an upstream carrier customer and/or a customer's customer is the subject of repeated traceback investigations, VERSCOM terminates the upstream carrier customer's ability to send any traffic for termination in the United States over the VERSCOM network and informs the upstream carrier that all United States terminating traffic will continue to be blocked until the carrier can establish to VERSCOM's satisfaction that it has removed the fraudulent robocall traffic from its network and that the carrier is committed to preventing and mitigating such traffic in the future.

VERSCOM LLC.

501 Silverside Street Suite
105 Wilmington DE 19809 USA
legal@verscom.com

II. Measures to Block Fraudulent Robocalls Identified by the FCC's Enforcement Bureau

VERSCOM is committed to cooperating with the Commission and its Enforcement Bureau in its effort to mitigate and block fraudulent robocalls. Where VERSCOM receives an inquiry from the Commission/ Enforcement Bureau related to suspicious or fraudulent robocall traffic traversing its network, it proceeds by:

1. Analyzing its call records to confirm that the suspicious or fraudulent robocall traffic identified was sent by the identified/alleged VERSCOM upstream carrier customer;
2. Confirming to the Commission/Enforcement Bureau that the information the Commission/Enforcement Bureau provided is correct and has been identified by VERSCOM, with a confirmation response time of 24 hours;
3. Reaching out to the upstream carrier customer to notify it of its anti-robocall rule violation and that, if further fraudulent robocall traffic originating from the carrier is identified, all U.S.-bound traffic transmitted by the customer with a +1 U.S.-originating number will be blocked unless the customer verifies the traffic is legitimate roaming traffic; and
4. Confirming with the Commission/Enforcement Bureau that VERSCOM has reached out to its upstream carrier customer, resolved the suspicious traffic at issue, and warned the customer that future violations will result in all U.S.-bound traffic transmitted by the customer with a +1 U.S.-originating number being blocked unless the customer verifies the traffic is legitimate roaming traffic.

VERSCOM is committed to responding fully and within 24 hours to all traceback requests from the Commission, civil and criminal law enforcement, and ITG and is prepared to modify its mitigation measures to individual inquiries/requests it receives from these entities. VERSCOM also requires its staff to cooperate with these entities to ensure compliance with all U.S. federal anti-robocalling and consumer protection laws.

In connection with the above, VERSCOM is also committed to fully complying with the Commission's robocall blocking requirements and confirms that it will block all calls and provider traffic that: (1) are identified in any public notice or order released by the Commission or (2) are substantially similar to the types of traffic identified in any public notice or order released by the Commission; or (3) include a caller ID number or name that is on the DNO list maintained by ITG.

III. Responding to Traceback Requests from the Commission, ITG, and Federal/State Authorities

VERSCOM fully complies with all requests made by law enforcement authorities or government agencies within 24 hours of their receipt and is committed to cooperating with these entities moving forward. Thus, in responding to traceback requests VERSCOM receives from the Commission, civil or criminal law enforcement, or ITG, it utilizes the processes identified in Section II above. VERSCOM similarly is prepared to modify its procedures to the individual directions included in any traceback request it receives. Moreover, to the extent VERSCOM is able to identify potentially fraudulent robocall traffic originating from one of its upstream carrier customers, it will notify ITG of this activity and thereafter work with ITG to resolve any issues that

VERSCOM LLC.

501 Silverside Street Suite
105 Wilmington DE 19809 USA
legal@verscom.com

arise. VERSCOM will similarly work to notify the Commission's Enforcement Bureau of fraudulent traffic through the Commission's Private Entity Robocall and Spoofing Portal. Where necessary, VERSCOM is willing to share with the necessary authorities the ALOC data VERSCOM gathers with respect to each of its upstream carrier customers sending calls for termination in the United States, so as to help these authorities in their efforts to identify and stop malicious and fraudulent traffic. VERSCOM maintains current and correct information about its upstream carrier customers so that it can provide accurate responses to traceback requests. VERSCOM maintains records of any traceback request it receives and the upstream carrier customer involved in the request.

VERSCOM will cooperate with state and federal regulators to prevent any and all illegal robocalls. Specifically, VERSCOM will:

- Respond to requests for information about illegal robocalls;
- Provide relevant non-proprietary information in response to reasonable and legitimate requests about illegal robocalls and suspicious activities; and
- Implement mandated robocall mitigation procedures to the fullest extent possible with the goal of maximizing the mitigation of illegal robocalls.

IV. STIR/SHAKEN Implementation

VERSCOM will comply fully with all conditions set forth in the FCC's orders, rules, and policies regarding the implementation of the STIR/SHAKEN framework for gateway providers and nongateway intermediate providers, including the various call authentication Reports and Orders and 47 C.F.R. § 64.6302(c), (d).

VERSCOM has implemented technical procedures to pass unaltered any identity header it receives with calls using Session Initiation Protocol (SIP) on the IP portions of its network to terminating voice service providers or subsequent intermediate providers in the call path.