



Massive Networks, Inc.

Robocall Mitigation Program

February 2024 Version

Primary Address:

382 S. Arthur #120
Louisville, CO 80027



Table of Contents

I.	Robocall Mitigation Program Introduction.....	3
A.	Company Summary.....	3
B.	Filing of RMP and Implementation of STIR/SHAKEN.....	4
II.	Robocall Mitigation Program	5
	1. Implementing Knowing Your Customer and Upstream Providers Protocols.....	5
	2. Requiring Contractual Provisions to Mitigate Illegal Robocalls.....	7
	3. Validating Customer's Right to Use Telephone Numbers	8
	4. Only Accepting Traffic from Providers that Have Affirmatively Filed in the RMD.....	8
	5. Analyzing and Monitoring Network Traffic Routing Through Massive Networks' Network.....	9
	6. Investigating Suspicious Calling Patterns.....	9
	7. Ensuring Foreign Providers Are Not Using Massive Networks to Carry or Process High-Volume Illegal Traffic onto the U.S. Network	10
	8. Authenticating Voice Traffic	10
	9. Responding to Commission, Law Enforcement and ITG Traceback Requests.....	10
	10. Designating an Employee Responsible for Addressing Robocall Mitigation-Related Issues.....	11
	11. Updates to Massive Networks' RMD Submission and RMP	11
	12. Employee Training	11



I. Robocall Mitigation Program Introduction

Pursuant to the applicable orders and regulations of the Federal Communications Commission ("FCC" or "Commission"), the following is the Robocall Mitigation Program ("RMP") that details the procedures of Massive Networks, Inc. ("Massive Networks"), a Colorado corporation, to prevent unlawful robocalls from originating, terminating, or being carried or processed where it is operating as a Voice Service Provider. Unless defined differently herein, capitalized terms used herein have the same definitions as set forth under 47 C.F.R § 64.6300.¹

A. Company Summary

Massive Networks is a leader in managed network services. At Massive Networks, we believe that our success is directly connected to the success of our partners and customers. As a global managed network provider, we are committed to delivering reliable, fast, and secure connectivity that empowers businesses to thrive in today's digital landscape. We ensure the security of our customer's network connections, data and privacy in every product and service we deliver to every customer.

With our One Vendor, One MSA, One Invoice, and One Pipe Multi-Connect® approach, we simplify the complexity of managing multiple vendors with desperate network issues to reduce operational expenses and cyber risks. Our focus on partnering and problem-solving ensures that we work in lock-step with our customer and partner teams to deliver faster time-to-value and ease of doing business with.

Whether a customer is a mid-market business looking to connect its offices, Internet, data centers, and cloud platforms or a partner looking to grow its business with us, Massive Networks has the expertise, resources, and solutions to help our customers achieve their goals.

¹ Within this RMP, Massive Networks has implemented rules established under the FCC's *Sixth Report and Order* along with its *Seventh Report and Order*. See *Advanced Methods to Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, *Seventh Report in Order* in CG Docket 17-59 and WC Docket 17-97 et al., [FCC 23-37](#), at Appendix A (rel. May 19, 2023) ("*Seventh Report and Order*"); *Advanced Methods to Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor*, WC Doc. No. 17-97, *Six Report in Order* and Notice of Proposed Rulemaking, [FCC 23-18](#), at Appendix A (rel. Mar. 19, 2023) ("*Sixth Report and Order*").



Massive Networks only serves as Voice Service Provider for this RMP. It is not an Intermediate Provider, Gateway Provider, Non-Gateway Intermediate Provider, Foreign Voice Service Provider or Foreign Intermediate Provider. Massive does not have an Operating Company Number ("OCN").

B. Filing of RMP and Implementation of STIR/SHAKEN

In submitting this RMP with the Commission, Massive Networks has certified that (a) all of the calls it originates on its network are subject to this RMP, (b) its prior certification has not been removed by Commission action, and (c) it has not been prohibited from filing in the Robocall Mitigation Database ("RMD") by the Commission.²

When providing voice services, Massive Networks only resells the Voice over Internet Protocol ("VoIP") services of PCI Broadband, which has a Robocall Mitigation Database No. RMD0007736 and FCC Registration Number ("FRN") of 0016286825 (referred to herein as "Wholesale Provider"). Therefore, as a reseller and pursuant to 47 C.F.R. § 64.6305(d)(1)(iii) and (2)(ii), Massive Networks has certified that it has "not implemented the STIR/SHAKEN authentication framework on any portion of its network" because it is "unable to implement STIR/SHAKEN due to a lack of control over the network infrastructure necessary to implement STIR/SHAKEN."³

Pursuant to 47 C.F.R. § 64.6305(d)(2)(ii) and (iii), Massive Networks' RMP, which has been uploaded into the RMD, reflects the "reasonable steps to avoid originating illegal robocall traffic" and includes "a commitment to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls."

Pursuant to 47 C.F.R. § 64.6305(d)(4)(vi)(3), Massive Networks' role in the call chain includes being:

- A Voice Service Provider without a STIR/SHAKEN implementation obligation serving end-users.

Pursuant to FCC Rule 64.6305(d)(2)(iv),⁴ Massive Networks states that that during the past two years, it (and/or any entity for which Massive Networks shares common ownership, management, directors, or control) has not been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to transmitting,

² 47 C.F.R. § 64.6305(d)(1).

³ 47 C.F.R. § 64.6305(d)(2)(i).

⁴ 47 C.F.R. § 64.6305(d)(2)(iv).



encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient RMD certification or RMP description.

II. Robocall Mitigation Program

This RMP applies to Massive Networks' VoIP services and provides information on the specific reasonable steps Massive Networks has taken to avoid originating, terminating, or carrying or processing illegal robocall traffic:

- (1) Implementing Knowing Your Customer and Upstream Provider Protocols
- (2) Requiring Contractual Provisions to Mitigate Illegal Robocalls
- (3) Validating Customer's Right to Use Telephone Numbers
- (4) Only Accepting Traffic from Providers that Have Affirmatively Filed in the RMD
- (5) Analyzing and Monitoring Network Traffic Routing Through Massive Networks' Network
- (6) Investigating Suspicious Calling Patterns
- (7) Ensuring Foreign Providers Are Not Using Massive Networks to Carry or Process High-Volume Illegal Traffic onto the U.S. Network
- (8) Authenticating Voice Traffic
- (9) Responding to Commission, Law Enforcement and ITG Traceback Requests within 24 Hours
- (10) Designating an Employee Responsible for Addressing Robocall Mitigation-Related Issues
- (11) Updating Massive Networks' RMD Submission and RMP
- (12) Training Employees

1. Implementing Knowing Your Customer and Upstream Providers Protocols

The FCC requires that a Voice Service Provider's RMP "describe with particularity" its robocall mitigation techniques as follows: (1) a Voice Service Provider must describe how it is meeting its existing obligation to take affirmative, effective measures to "know its customers" and prevent new and renewing customers from originating illegal calls; and (2) Voice Service Provider must describe any "know-your-upstream provider" procedures in place designed to mitigate illegal robocalls.⁵ To comply with the requirements to describe their "new and renewing customer" and "know-your-upstream provider" procedures, such providers must describe any contractual provisions with end-users or upstream providers designed to mitigate illegal

⁵ See 47 C.F.R. § 64.6305(d)(2)(ii); see also *Sixth Report and Order*, FCC 23-18, ¶ 40; *Seventh Report and Order*, FCC 23-37, ¶¶ 3 & 49.



robocalls.⁶ Massive Networks' contractual provisions with its customers are described in Section 2 below.

Massive Networks has implemented Know Your Customer procedures used when onboarding new or renewing customers to ensure that such customers and providers do not or are not likely to engage in any prohibited conduct. When signing up new end user customers that will receive its VoIP services, Massive Networks appropriately collects information about a subscriber to determine that subscriber's "identity and operational legitimacy."⁷ For instance, as part of the vetting process, Massive Networks generally requires its customers to provide the full legal name of the company, state or country of incorporation, the physical address of its operations, the billing name and address (when different), and the customer contact name and telephone number, nature of the customer's business, among other things. Doing so is necessary to provide a prompt response to traceback requests and enforcement efforts.

As a reseller, because Massive Networks is a reseller of VoIP services and therefore, lacks the control over the network infrastructure necessary to implement STIR/SHAKEN, Massive Networks relies on its Wholesale Provider to satisfy the Know Your Upstream Provider obligations, as well as ensure, per Section 4 below, the Wholesale Provider's upstream providers are appropriately listed in the FCC's RMD and

⁶ See *Sixth Report and Order*, ¶ 40 and n.154 (explaining that "[w]e do not expect providers to necessarily submit contractual provisions, but to describe them in general terms, including whether such provisions are typically included in their contracts."); *Seventh Report and Order*, FCC 23-37, ¶¶ 3 & 49 (explaining that "[i]n general, we expect voice service providers will need to exercise due diligence before accepting traffic from an upstream provider, and may want to collect information such as 'obtaining the [voice service provider's] physical business location, contact person(s), state or country of incorporation, federal tax ID (if applicable), and the nature of the [voice service provider's] business. We do not find that collecting this information is either uniformly necessary or sufficient, and voice service providers may need to take additional steps, such as adopting contract terms that allow for termination and acting on those terms in the event that the upstream provider attempts to use the network to carry or process a high volume of illegal traffic.'" While the Commission "do[es] not expect perfection," "all voice service providers must take effective steps, and if a voice service provider carries or transmits a high volume of illegal traffic that primarily originates from one or more specific upstream providers, the steps that provider has taken are not effective and must be modified for that provider to be in compliance with our rules.").

⁷ *Wireline Competition Bureau Issues Caller ID Authentication Best Practices*, WC Docket Nos. 17-97 and 20-324, DA 20-1526, Public Notice, ¶ 12 & n.35 (rel. Dec. 22, 2020) ("FCC's Caller ID Authentication Best Practices"), available at <https://docs.fcc.gov/public/attachments/DA-20-1526A1.pdf>.



have not been delisted pursuant to an enforcement action before accepting traffic from the provider.

With these measures along with those discussed in Section 3, below and Massive Networks' role as a reseller of its Whole Provider's VoIP services, Massive Networks takes "affirmative, effective measures to [(1)] prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal traffic"⁸ and (2) know its upstream providers.⁹

2. Requiring Contractual Provisions to Mitigate Illegal Robocalls

In satisfaction of the FCC's requirements that a provider "know its customers"¹⁰ procedures, below are descriptions of Massive Networks' contractual provisions with end-users that are designed to mitigate illegal robocalls.

Massive Networks' voice service customers are subject to its [Acceptable Use Policy](#) ("AUP"), which includes provisions that prohibit customers from using Massive Networks' services in a manner which "[v]iolates any applicable law, regulation, treaty, or tariff."¹¹ Under the AUP, Massive Networks "expressly reserves the right, at its discretion, to pursue any remedies that it believes are warranted which may include, but is not limited to, the issuance of written or verbal warnings, filtering, blocking, suspending, or terminating accounts, billing Customer for administrative costs and/or reactivation charges or bringing legal action to enjoin violations and/or to collect damages, if any, caused by Customer violations."¹² Under its AUP, Massive Networks has the right to change the AUP with notice by publication on its website. Massive Network's Master Service Agreement with its customers incorporates this AUP by reference and also specifies that Massive Networks may immediately interrupt, restrict, suspend or discontinue providing Service for violations of the AUP.

⁸ 47 C.F.R. § 64.1200(n)(4).

⁹ See also 47 C.F.R. § 64.6305(d)(2)(ii).

¹⁰ 64.6305(d)(2)(ii) (which cites the obligation under 47 C.F.R. § 64.1200(n) to "[t]ake affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal traffic.").

¹¹ See AUP.

¹² *Id.*



3. Validating Customer's Right to Use Telephone Numbers

When Massive Networks establishes service to a retail end user voice customer, Massive Networks confirms the end user customer has a verified association with the telephone numbers it uses for its originating telephone calls. In this connection, Massive Networks either assigns the telephone numbers to its VoIP end user customers or ports an existing end user's customer telephone number Massive Networks' VoIP service.

In addition, when using Massive Networks' VoIP service offering, its customers have limited means to simultaneously send numerous calls over a few voice paths. For these reasons, Massive Networks does not consider its customers to be a high risk of originating illegal robocalls or spoofed calls on Massive Networks' network. Nevertheless, Massive Networks has adopted various measures discussed below to prevent the origination of such calls on its network.

4. Only Accepting Traffic from Providers that Have Affirmatively Filed in the RMD

In accordance with FCC rules referenced below and because Massive Networks is a reseller of VoIP services and therefore, lacks the control over the network infrastructure necessary to implement STIR/SHAKEN, Massive Networks relies on its Wholesale Provider, which is currently listed in the RMD, to only accept traffic from providers that at a minimum satisfy the following requirements:

- Accepting traffic from domestic Voice Service Providers. In accordance with 47 C.F.R § 64.6305(g)(1), Massive Networks accepts calls directly from a domestic Voice Service Provider only if that Voice Service Provider's filing appears in the RMD and that filing has not been de-listed pursuant to an enforcement action.
- Accepting traffic from Foreign Voice Service Providers or Foreign Intermediate Providers. In accordance with 47 C.F.R § 64.6305(g)(2), Massive Networks accepts calls from Foreign Voice Service Providers or Foreign Intermediate Providers that use NANP resources that pertain to the U.S. in the caller ID field to send voice traffic to residential or business subscribers in the U.S., only if that foreign provider's filing appears in the RMD in accordance with paragraph and that filing has not been de-listed pursuant to an enforcement action.
- Accepting traffic from Gateway Providers. In accordance with 47 C.F.R § 64.6305(g)(3), Massive Networks accepts calls directly from a Gateway Provider only if that Gateway Provider's filing (a) appears in the RMD, (b) shows that the Gateway Provider has affirmatively submitted the filing, and (c) has not been de-listed pursuant to an enforcement action.



- Accepting traffic from Non-Gateway Intermediate Providers. In accordance with 47 C.F.R § 64.6305(g)(4) and its effective date, Massive Networks accepts calls directly from a Non-Gateway Intermediate Provider only if that Non-Gateway Intermediate Provider's filing (a) appears in the RMD, (b) shows that the Non-Gateway Intermediate Provider has affirmatively submitted the filing, and (c) has not been de-listed pursuant to an enforcement action.

5. Analyzing and Monitoring Network Traffic Routing Through Massive Networks' Network

Because Massive Networks is a reseller of VoIP services and therefore, lacks the control over the network infrastructure necessary to implement STIR/SHAKEN, Massive Networks relies on its Wholesale Provider to analyze and monitor high-volume voice traffic for patterns consistent with robocalls. As a reseller, Massive Networks does not use a third-party analytics vendor(s).

As discussed in Section 6, below, if suspicious calling patterns are found by its Wholesale Provider to be originating from a Massive Network customer, Massive Networks, after further investigation, will take appropriate action to address such behaviors. If the calls are determined to be illegal robocalls originating from a Massive Networks' customer, Massive Networks' service to the customer originating such calls will be suspended or terminated, as discussed in Section 2, above. If the robocalls are illegal and terminating to Massive Networks' customers, Massive Networks will, when necessary and appropriate, work with its Wholesale Provider to address and block such traffic.

6. Investigating Suspicious Calling Patterns

Because Massive Networks is a reseller of VoIP services and therefore, lacks the control over the network infrastructure necessary to implement STIR/SHAKEN, Massive Networks relies on its Wholesale Provider to monitor and detect calling patterns consistent with or specific to illegal robocalls (including large bursts of traffic in small timeframes, low duration subscriber traffic and sequential dialing patterns, or call pattern that is consistent with illegal robocalls). If its Wholesale Provider has good reason to suspect illegal robocalling or illegal spoofing is originating from a Massive Networks' customer, Massive Networks' voice services to its customer will be investigated and suspended or terminated, as appropriate and in accordance with Massive Networks' AUP discussed in Section 2, above. If the robocalls are illegal and terminating to a VoIP customer of Massive Networks, it will, when necessary and appropriate, work with its Wholesale Provider to address and block such traffic. To ensure that Massive Networks' customers are protected from illegal and potentially fraudulent call traffic, and consistent with contractual limitations and legal considerations, Massive Networks takes these



appropriate steps to combat such traffic being originated, terminated, or carried or processed via its VoIP service offering.

7. Ensuring Foreign Providers Are Not Using Massive Networks to Carry or Process High-Volume Illegal Traffic onto the U.S. Network

Pursuant to 47 C.F.R. § 64.1200(n)(5), Massive Networks takes reasonable and effective steps discussed under Sections 1-6, above, to ensure that “any originating provider or intermediate provider, foreign or domestic, from which it directly receives traffic is not using the provider to carry or process a high volume of illegal traffic onto the U.S. network.”

8. Authenticating Voice Traffic

Because Massive Networks is a reseller and therefore, lacks the control over the network infrastructure necessary to implement STIR/SHAKEN, Massive Networks relies on its Wholesale Provider to comply with 47 C.F.R. § 64.6301(a), which involves (1) authenticating and verifying caller identification information for all SIP calls that exclusively transit its own network; (2) Authenticating caller identification information for all SIP calls it originates and that it will exchange with another Voice Service Provider or Intermediate Provider and, to the extent technically feasible, transmit that call with authenticated caller identification information to the next Voice Service Provider or Intermediate Provider in the call path; and (3) verifying caller identification information for all SIP calls it receives which it will terminate and for which the caller identification information has been authenticated.

9. Responding to Commission, Law Enforcement and ITG Traceback Requests

Massive Networks has been and is committed to fully and timely responding to all such traceback requests from the Commission, law enforcement, and the industry traceback consortium/group (ITG), and will continue to cooperate with such entities in investigating and stopping illegal robocallers that use Massive Networks’ services and network is not utilized for the origination, termination or routing of unwanted and illegal robocalls. In accordance with the FCC’s regulations 47 C.F.R. § 64.1200(n)(1) along with 47 C.F.R. § 64.6305(a)(2) and (d)(2)(iii), Massive Networks will respond to all traceback requests from the Commission, law enforcement, and the ITG well within 24 hours¹³ and will cooperate with such entities in investigating and stopping any illegal robocallers that attempt to use Massive Networks’ network and/or services to originate calls. Massive Networks will take the steps to effectively mitigate illegal traffic when it receives actual

¹³ This is 24-hour window applies within business days, per rule 47 C.F.R. § 64.1200(n)(1)(ii) and as clarified by the Commission. See *a/so* FCC 22-37, at n.211.



written notice of such traffic from the Commission through its Enforcement Bureau and will comply with the requirements of such notice and do so in accordance with the applicable FCC rules.¹⁴

10. Designating an Employee Responsible for Addressing Robocall Mitigation-Related Issues

To further ensure Massive Networks' network is not utilized for the origination, termination, or carrying or processing of unwanted and illegal robocalls, Massive Networks provides the following name, title, department, business address, telephone number, and email address of the individual within Massive Networks that handles robocall mitigation-related issues as well as responds to traceback inquiries from the FCC, ITG, and law enforcement agencies:

Contact Name:	James Coberly
Contact Title:	CTO/COO
Contact Department:	Main Office
Contact Street Address:	382 S. Arthur #120
Contact City:	Louisville
Contact State and Zip Code:	Colorado 80027
Contact Telephone Number:	(303) 800-1300
Contact Email:	jcoberly@massivenetworks.com

11. Updates to Massive Networks' RMD Submission and RMP

Consistent with FCC Regulations, 47 C.F.R. § 64.6305(d)(5), Massive Networks will update its submission in the RMD within 10 business days of any change to the applicable information it must provide and update in the RMD.

12. Employee Training

Finally, it is Massive Networks' policy that employees responsible for combating robocalling are educated on the Massive Networks' RMP along with any related implementing procedures and stay appropriately apprised of the latest developments and emerging trends to combat illegal robocalling. Massive Networks treats this continuing education as a critical piece of its role in the telecommunications ecosystem and its strategic position as a partner in mitigating illegal traffic.

¹⁴ See 47 C.F.R. § 64.1200(n)(2) and (3).