



thinQ Technologies, Inc. d/b/a Commio

Robocall Mitigation Program

April 2025 Version

Primary Address:

5420 Wade Park Blvd.
Suite 100
Raleigh, NC 27607



Table of Contents

I.	Robocall Mitigation Program Introduction	3
A.	Company Summary	3
B.	Filing of RMP and Implementation of STIR/SHAKEN	3
II.	Robocall Mitigation Program.....	4
	1. Implementing Knowing Your Customer and Upstream Providers Protocols.....	5
	2. Requiring Contractual Provisions to Mitigate Illegal Robocalls	6
	3. Validating Customer's Right to Use Telephone Numbers	7
	4. Blocking Calls on a Do-Not-Originate List	8
	5. Only Accepting Traffic from Providers that Have Affirmatively Filed in the RMD	8
	6. Analyzing and Monitoring Network Traffic Routing Through Commio's Network	9
	7. Investigating Suspicious Calling Patterns.....	9
	8. Ensuring Foreign Providers Are Not Using Commio to Carry or Process High-Volume Illegal Traffic onto the U.S. Network	9
	9. Authenticating Voice Traffic.....	10
	10. Responding to Commission, Law Enforcement and ITG Traceback Requests within 24 Hours.....	10
	11. Designating an Employee Responsible for Addressing Robocall Mitigation-Related Issues	11
	12. Updating Commio's RMD Submission and RMP	11
	13. 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 thinQ Technologies, Inc. d/b/a Commio’s (“Commio”) Robocall Mitigation Program (“RMP”) that it established to prevent unlawful robocalls from originating, terminating, or being carried or processed on Commio’s voice network where it is operating as a Voice Service Provider, Gateway Provider, or Non-Gateway Intermediate 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

Commio is an innovative VoIP provider focused on providing better voice and messaging solutions to eliminate worry, unnecessary costs, and complexity. Commio is a North Carolina Corporation, and its Operating Company Numbers (“OCNs”) are 939H and 022H.

Depending on the services being provided, Commio may serve as a Voice Service Provider, Gateway Provider, or Non-Gateway Intermediate Provider to commercial customers. In addition, Commio does not serve residential customers.

B. Filing of RMP and Implementation of STIR/SHAKEN

In submitting this RMP with the FCC, Commio states that: (a) all of the calls it originates, carries or processes 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

Pursuant to 47 C.F.R. § 64.6305(d)(1)(i), (e)(1)(i) and (f)(1)(i), Commio has also certified that it has fully implemented STIR/SHAKEN across its network and all calls it originates, carries or processes are compliant with 47 C.F.R. §§ 64.6301(a)(1) and (2), and 64.6302(b).

Pursuant to 47 C.F.R. § 64.6305(d)(2)(ii) and (iii), (e)(ii) and (iii), and (f)(ii) and (iii),

¹ Within this RMP, Commio 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*”).

² 47 C.F.R. § 64.6305(d)(1), (e)(1), and (f)(1).



Commio's RMP, which has been uploaded into the RMD, reflects the "reasonable steps to avoid originating[, carrying or processing] 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[, carry or process] calls."

Pursuant to 47 C.F.R. § 64.6305(d)(4)(vi), (e)(4)(vi), and (f)(4)(vi), Commio's role in the call chain includes being:

- A Voice Service Provider with a STIR/SHAKEN implementation obligation serving end-users;
- A Voice Service Provider with a STIR/SHAKEN obligation acting as a wholesale provider originating calls on behalf of another provider or providers;
- A Gateway Provider with a STIR/SHAKEN obligation; and
- A Non-Gateway Intermediate Provider with a STIR/SHAKEN obligation.

II. Robocall Mitigation Program

This RMP applies to Commio's calling platforms (which are all IP-based) and provides information on the following topics³ that are discussed in turn below which detail the specific reasonable steps Commio 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) Blocking Calls on a Do-Not-Originate List
- (5) Only Accepting Traffic from Providers that Have Affirmatively Filed in the RMD
- (6) Analyzing and Monitoring Network Traffic Routing Through Commio's Network
- (7) Investigating Suspicious Calling Patterns
- (8) Ensuring Foreign Providers Are Not Using Commio to Carry or Process High-Volume Illegal Traffic onto the U.S. Network
- (9) Authenticating Voice Traffic
- (10) Responding to Commission, Law Enforcement and ITG Traceback Requests within 24 Hours
- (11) Designating an Employee Responsible for Addressing Robocall Mitigation-Related Issues
- (12) Updating Commio's RMD Submission and RMP
- (13) Training

³ Commio has various supporting policies and procedures that implement various aspects of this RMP.

1. Implementing Knowing Your Customer and Upstream Providers Protocols

The FCC requires that a Voice Service Provider's, Gateway Provider's, and Non-Gateway Intermediate Provider's RMPs "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) a Gateway Provider, Non-Gateway Intermediate Provider and Voice Service Provider must describe any "know-your-upstream provider" procedures in place designed to mitigate illegal robocalls.⁴ 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 robocalls.⁵ Commio's contractual provisions with its commercial customers are described in Section 2 below.

Commio has implemented Know Your Customer and Upstream Provider Policy and 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. As indicated in Section 5, below, if the customer is a Voice Service Provider, Gateway Provider, Non-Gateway Intermediate Provider, Foreign Voice Service Provider, and/or Foreign Intermediate Provider, Commio confirms that the provider is appropriately listed in the FCC's RMD and has not been delisted pursuant to an enforcement action before accepting traffic from the provider.

⁴ See 47 C.F.R. §§ 64.6305(d)(2)(ii), (e)(2)(ii) and (f)(2)(ii); see also *Sixth Report and Order*, FCC 23-18, ¶ 40; *Seventh Report and Order*, FCC 23-37, ¶¶ 3 & 49.

⁵ See *Sixth Report and Order*, FCC 23-18, ¶ 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.").

Consistent with the FCC’s Caller ID Authentication Best Practices No. 1⁶ and 47 C.F.R. § 64.1200(n)(4), Commio vets, among other things, “the identity of retail and wholesale subscribers, in conjunction with (i) approving an application for service; (ii) provisioning of network connectivity; (iii) entering into a contract agreement; or (iv) granting the right-to-use telephone number resources.”⁷ In so doing, Commio 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 below are descriptions of Commio’s contractual provisions with end-users that are designed to mitigate illegal robocalls.

Commio’s commercial voice service customers are subject to robust terms and conditions that (1) obligate customers not to use Commio’s services for unlawful purposes; and (2) preserve Commio’s right to terminate customers for violations of the law. In particular, Commio mandates that each agreement with its customers incorporates Commio’s Acceptable Use Policy (“AUP”), which includes, among other things, a termination clause for violations of any law or regulation applicable to the customer’s use of Commio’s services or its equipment. Commio also retains the right to immediately suspend or terminate service without notice for violations of its AUP, which prohibits the use of Commio’s network, machines, or services in any manner that:

- violates any applicable law, regulation, treaty, or tariff, including but not limited to data privacy laws and laws restricting or prohibiting unlawful robocalls, telemarketing calls or messages, use of auto dialers;
- violates the acceptable use policies of any networks, machines, or services which are accessed through Commio’s network;
- violates the privacy of others;
- involves deceptive online marketing practices including, without limitation,

⁶ *Wireline Competition Bureau Issues Caller ID Authentication Best Practices*, WC Docket Nos. 17-97 and 20-324, DA 20-1526, at Appendix A (rel. Dec. 22, 2020) (“FCC’s Caller ID Authentication Best Practices”), available at <https://docs.fcc.gov/public/attachments/DA-20-1526A1.pdf>.

⁷ *Id.*

⁸ 47 C.F.R. §§ 64.1200(n)(4) and 64.6305(d)(2)(ii).

⁹ See also 47 C.F.R. §§ (d)(2)(ii), (e)(2)(ii), and (f)(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.”).



practices that violate the United States Federal Trade Commission's guidelines for proper online marketing or telemarketing;

- involves the use or transmission of fraudulent traffic or fraudulent activity, including without limitation call spoofing, traffic pumping fraud, and fraudulent bot traffic;
- falsifies, manipulates, spoofs, or otherwise tampers with user identification information and/or caller identification information;
- fails to authenticate call traffic in accordance with applicable laws and regulations;
- furnishes false or incorrect data or information to Commio, including without limitation information provided on signup, Know-Your-Customer forms, or otherwise in response to any request by Commio to ascertain or verify the customer's identity and business practice; or
- impersonates or misrepresents the customer's affiliation with any person or entity.

Further, Commio's AUP requires all customers to comply with the Telephone Consumer Protection Act and its implementing regulations, the Telemarketing Sales Rule, regulations implementing the FCC's national Do-Not-Call registry, and all other rules and regulations governing the sending of telemarketing calls and/or robocalls. Commio's customers that are Communications Services Providers ("CSPs") which provide services to their own customers are made responsible for compliance with the AUP by such customers and are obligated by the AUP to take steps to ensure such compliance.

In addition, Commio reserves the right to suspend or terminate service without notice, if the AUP or applicable law is violated. In such instances, Commio will discontinue service without notice and/or seek legal recourse to recover all costs involved in enforcement.

3. Validating Customer's Right to Use Telephone Numbers

Pursuant to Commio's AUP, Commio's customers (both End Users and Communications Service Providers, *i.e.*, resellers) must be authorized to use the telephone numbers they associate with originating telephone calls. Any violation of Commio's AUP can ultimately result in termination or suspension of service. In addition, when onboarding new customers, Commio utilizes a Letter of Authorization process whereby the customer enters pertinent information into Commio's portal (pdf version is required for toll-free numbers). Commio then sends that information to the losing provider to validate that the information is correct, and the losing provider then checks with its customer to make sure that customer did in fact authorize the change in providers. If any of the information does not match, the losing provider will reject the change before it seeks confirmation from the customer in most cases.

4. Blocking Calls on a Do-Not-Originate List

When routing traffic as Gateway Provider, Commio blocks calls in accordance with FCC Rule 47 C.F.R. § 64.1200(o)(1)-(4) purporting to originate from a number on a reasonable Do-Not-Originate (“DNO”) list that is associated with North American Numbering Plan (“NANP”) numbers. Commio has protocols in place to detect DNO calls and blocks calls that are determined to originate from a DNO number. When serving as a Voice Service Provider Commio may, in accordance with FCC Rule 47 C.F.R. § 64.1200(k)(2), block such calls along with calls that Commio identifies, based on reasonable analytics, as highly likely to be associated with a one-ring scam.

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

In accordance with FCC rules referenced below, Commio only accepts 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), Commio 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), Commio 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), Commio 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, Commio 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.

Commio's Know Your Customer and Upstream Provider Policy and Procedures involve checking the RMD to see if the Provider's filing (a) appropriately appears in the RMD, (b) shows that the Provider has submitted the filing, and (c) has not been de-listed pursuant to an enforcement action.

6. Analyzing and Monitoring Network Traffic Routing Through Commio's Network

Upon receiving call traffic, Commio also analyzes and monitors the call traffic that originates, terminates, or is carried or processed on Commio's voice network. Commio does not use a third-party analytics vendor(s). It is Commio's policy to extract call traffic data on a daily basis to flag any suspicious activity. Activity is flagged as suspicious based on analysis of (a) call length and call count patterns, (b) cancel/86 reports, (c) 503 reports, (d) SIP data, and (e) other data sets based on known carrier algorithm performance.

Where suspicious activity is detected, Commio takes further steps to investigate the activity, including (a) in-depth review by the Commio engineering team to better understand the cause of the suspicious activity, (b) direct contact with the customer or carrier partner to address and mitigate the activity, (c) run reporting and closely watch the specific customer's activity to ensure the call traffic is valid, (d) investigate with the Industry Traceback Group if the customer is in good standing as a provider or otherwise has no open tickets or concerns; and/or (e) such other investigation as determined to be appropriate in Commio's discretion.

As discussed in Section 7, below, if suspicious calling patterns are found, Commio, after further investigation, takes appropriate action to address such behaviors, including terminating the customers service or blocking the calls.

7. Investigating Suspicious Calling Patterns

When analyzing and monitoring call traffic, if Commio discovers call patterns that are consistent with illegal robocalling, Commio, after further investigation, takes appropriate action to address such behaviors. Depending on the severity of the conduct and the information/explanation provided by the customer, corrective measures may include (a) suspension, (b) termination, (c) warnings to the customer and efforts to bring the customer within the terms of the governing contract terms and AUP, (d) throttling traffic, (e) reporting the customer to authorities, where call traffic is confirmed as illegal and potentially damaging to consumers, (f) additional monitoring, and/or (g) such other actions as deemed appropriate in the discretion of Commio, and consistent with law, regulations, and the governing contract(s) and Commio's AUP.

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

Pursuant to 47 C.F.R. § 64.1200(n)(5), Commio takes reasonable and effective steps discussed under Sections 1-7, 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."

9. Authenticating Voice Traffic

Pursuant to 47 C.F.R. § 64.6301(a), when operating as a Voice Service Provider, Commio does the following (1) Authenticates and verifies caller identification information for all SIP calls that exclusively transit its own network; (2) Authenticates 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) Verifies caller identification information for all SIP calls it receives from another Voice Service Provider or Intermediate Provider which it will terminate and for which the caller identification information has been authenticated.

Pursuant to 47 C.F.R. § 64.6302(c), when operating as a Gateway Provider, Commio “authenticate[s] caller identification information for all calls it receives that use NANP resources that pertain to the U.S. in the caller ID field and for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call, unless that Gateway Provider is subject to an applicable extension in § 64.6304.

Pursuant to 47 C.F.R. § 64.6302(d), when operating as a Non-Gateway Intermediate Provider, Commio “authenticate[s] caller identification information for all calls it receives directly from an originating provider and for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call.”

10. Responding to Commission, Law Enforcement and ITG Traceback Requests within 24 Hours

Commio is committed to ensuring that its network is not utilized for the origination, termination, or carrying or processing 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), (c)(2), (d)(2)(iii), (e)(2)(iii), and (f)(2)(iii), Commio will respond to all traceback requests from the Commission, law enforcement, and the Industry Traceback Consortium (“ITG”) within 24 hours¹¹ and will cooperate with such entities in investigating and stopping any illegal robocallers that attempt to use Commio’s network and services to originate, carry or process calls. Commio will take the steps to effectively mitigate illegal traffic when it receives actual 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.¹²

¹¹ This is 24-hour window applies within business days, per rule 47 C.F.R. § 64.1200(n)(1) and as clarified by the Commission. See also [FCC 22-36](#), at n.211.

¹² See 47 C.F.R. § 64.1200(n)(2) and (3).



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

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

Contact Name:	Kristen Broome
Contact Title:	Chief Financial Officer
Contact Business Address:	5420 Wade Park Blvd, Suite 100
Contact City:	Raleigh
Contact State and Zip Code:	North Carolina, 27607
Contact Telephone Number:	(919) 890-0000
Contact Email:	legal@commio.com

12. Updating Commio's RMD Submission and RMP

Consistent with FCC Regulations, 47 C.F.R. § 64.6305(d)(5), (e)(5) and (f)(5), Commio 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.

13. Training

Finally, Commio has implemented a training program that focuses on ensuring that personnel receive appropriate training on issues related to illegal robocalls. It is Commio's policy that all management-level employees maintain a robust continuing education program to assure they are up to date on (a) the Company's RMP along with the associated policies and procedures that implement the RMP, and (b) latest key developments and emerging trends involving: (1) scam and fraudulent traffic and patterns to look out for, (2) regulatory requirements on carriers and carrier partners, (3) robocall mitigation efforts, (4) law enforcement and legal activity related to domestic and international calling practices, (5) legal efforts, authorizations or requirements to identify, monitor, block or limit certain calls, (6) industry concerns regarding call monitoring, blocking, labeling, and/or reporting; (7) call identification and authentication protocols and requirements; and (8) the broader legal framework applicable to Commio's operations. Commio treats this continuing legal education as a critical piece of its role in the telecommunications ecosystem and its strategic position as a partner in mitigating illegal traffic.