

# **Robocall Mitigation Program**

September 2023

## **I. Robocall Mitigation Program Introduction**

Pursuant to the applicable orders and regulations of the Federal Communications Commission (“FCC” or “Commission”), the following Robocall Mitigation Program (“RMP”) details the policies and practices that Gizat Global Communications LTD. (“Gizat”), FRN 0033876236 was established to prevent unlawful robocalls from originating on, terminating to, or routing through its voice network where it is operating as a Voice Service Provider, Gateway Provider, or Intermediate Provider. Unless defined differently herein, capitalized terms used herein have the same definitions as set forth under 47 C.F.R § 64.6300.

### **A. Company Summary**

Gizat is a global provider of cloud communications and VOIP communications services. Its businesses make it easier for businesses to connect, support and share across international borders. With its commercial offerings, Gizat enables businesses to transact and communicate with their customers with enhanced intelligence and insight. As indicated above, depending on the services provided, Gizat may serve as a Voice Service Provider, an Intermediate Provider, and/or a Gateway Provider.

### **B. Filing of RMP and Implementation of STIR/SHAKEN**

GIZAT has fully implemented STIR/SHAKEN and has submitted its certification that all voice traffic that originates on its network is authenticated with STIR/SHAKEN consistent with 47 C.F.R. § 64.6301(a)<sup>2</sup>. In accordance with the RMD 12/2022 Filing Instructions, FCC Rule 47 C.F.R. § 64.6305(b)<sup>3</sup> and because Gizat is a “Combined Gateway and Voice Service Provider” under these instructions, Gizat has certified that Gizat has “fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it carries or processes are compliant with FCC Rule, 47 C.F.R. § 64.6302(b).”<sup>4</sup> In addition, Gizat has uploaded this RMP into the RMD because it “details the specific reasonable steps it has taken to avoid carrying or processing illegal robocall traffic” and has included “a commitment to respond fully and 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 carry or process calls.”<sup>3</sup>

---

<sup>1</sup> See Robocall Mitigation Database External Filing Instructions, Version: December 2022 (“RMD 12/2022 Filing Instructions”), available at <https://www.fcc.gov/sites/default/files/rmd-instructions.pdf>.

## II. Robocall Mitigation Program

This RMP applies to Gizat calling platforms and provides information on Gizat policies and procedures on the following topics that are discussed in turn below which “details the specific reasonable steps [IP Link] has taken to avoid carrying or processing illegal robocall traffic”:

- (1) Implementing Knowing Your Customer Protocols
- (2) Requiring Contractual Provisions to Mitigate Illegal Robocalls
- (3) Blocking Calls on a Do-Not-Originate List
- (4) Analyzing and Monitoring Network Traffic Routing
- (5) Ensuring Foreign Providers Are Not Using Gizat to Carry or Process High-Volume Illegal Traffic onto the U.S. Network
- (6) Authenticating Voice Traffic Originated by Gizat
- (7) Responding to Commission, Law Enforcement and ITG Traceback Requests
- (8) Designating an Employee Responsible for Addressing Robocall Mitigation-Related Issues
- (9) Updating our RMD Submission and RMP

---

<sup>4</sup> 47 C.F.R. § 64.6302(b) (stating that Intermediate Provider shall “[a]uthenticate caller identification information for all calls it receives for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call, except that the intermediate provider is excused from such duty to authenticate if it: (1) Cooperatively participates with the industry traceback consortium; and (2) Responds fully and in a timely manner to all traceback requests it receives from the Commission, law enforcement, and the industry traceback consortium regarding calls for which it acts as an intermediate provider”).

<sup>5</sup> RMD 12/2022 Filing Instructions at 12-13. *See also* 47 C.F.R. § 64.6305(d)(2)(ii) (even if a gateway provider is fully compliance with STIR/SHAKEN, it must file an RMP that sets forth “[t]he specific reasonable steps the gateway provider has taken to avoid carrying or processing illegal robocall traffic as part of its robocall mitigation program, including a description of how it has complied with the know-your-upstream provider requirement in § 64.1200(n)(4)”).

## **1. Implementing Knowing Your Customer Protocols**

Consistent with the FCC’s Caller ID Authentication Best Practices No. 1<sup>6</sup> and 47 C.F.R. § 64.1200(n)(3), Gizat vets “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.”<sup>7</sup> In so doing, Gizat takes “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.”<sup>8</sup>

In this regard, Gizat has implemented appropriate Know Your Customer (“KYC”) protocols when onboarding new or renewing customers. As part of its KYC protocols, Gizat requires any customer to provide sufficient information to ensure its legitimacy. Among other things, Gizat 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, and nature of the customer’s business. As indicated in Section 3, below, if the company is a Voice Service Provider, Foreign Voice Service Provider, Intermediate Provider, and/or Gateway Provider, Gizat confirms, in accordance with currently effective FCC rules, that the company is appropriately listed in the FCC’s RMD and has not been delisted pursuant to an enforcement action before accepting traffic from such entities.<sup>9</sup>

## **2. Requiring Contractual Provisions to Mitigate Illegal Robocalls**

Voice service customers of Gizat are subject to robust terms and conditions that (1) obligate customers not to use the services for unlawful purposes; and (2) preserve GIZAT right to terminate customers for violations of the law.

Gizat’s contracts include terms that forbid the customer from using our services to originate and/or otherwise transmit calls that violate laws restricting robocalls or other telemarketing calls, including the federal Telephone Consumer Protection Act (“TCPA”) and/or the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (“TRACED Act”) and/or the rules promulgated pursuant to these statutes. Gizat’s contract terms provide that if any calls originated or otherwise transmitted by the customer to Gizat violate the TCPA, the TRACED Act, or the rules promulgated under these statutes, then Gizat may, at its sole discretion, suspend or terminate the customer’s service immediately, among other remedies.

---

<sup>6</sup> 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>.

<sup>7</sup> *Id.*

<sup>8</sup> 47 C.F.R. § 64.1200(n)(3).

<sup>9</sup> See 47 C.F.R. § 64.6305(e)(1)-(3).

### **3. Blocking Calls on a Do-Not-Originate List**

In accordance with FCC Rules, 47 C.F.R. § 64.1200(k)(2) and (o)(1)-(4), Gizat blocks calls purporting to originate from a number on a reasonable Do-Not-Originate (“DNO”) list that is associated with North American Numbering Plan numbers.

### **4. Analyzing and Monitoring Network Traffic**

Upon receiving call traffic, Gizat also analyzes and monitors the call traffic that originates on, terminates to, or routes through the voice network.

In this regard, Gizat has in place anti-fraud processes that enable it to, among other things, monitor network usage, identify suspicious network activity (based on call duration, abnormal call patterns, atypical call activity, and subscriber information), receive automatic alerts, investigate traffic to distinguish fraud from honest customer usage, and resolve cases intelligently on a case-by-case basis. When analyzing and monitoring call traffic, if Gizat discovers call patterns that are consistent with illegal robocalling, Gizat, after further investigation, takes appropriate action to address such behaviors, which may include working with the originating customer to resolve problematic traffic, blocking the problematic calls and/or terminating the customer’s service.

### **5. Ensuring Foreign Providers Are Not Using Gizat to Carry or Process High-Volume Illegal Traffic onto the U.S. Network**

Pursuant to 47 C.F.R. § 64.1200(n)(4) and its January 16, 2023 effective date, when Gizat serves as a Gateway Provider for voice traffic that is routing through its network, Gizat takes reasonable and effective steps discussed under Section 5, above, to ensure that any Foreign Voice Service Provider or Foreign Intermediate Provider from which Gizat directly receives traffic is not using Gizat, as a Gateway Provider, to carry or process a *high volume* of illegal traffic onto the U.S. network. In addition, as a Gateway Provider, Gizat blocks – to the best of its ability – foreign originating calls with U.S. North American Numbering Plan numbers in the Caller ID, unless the upstream provider has been previously approved for sending such traffic, based on satisfactory due diligence.

### **6. Authenticating Voice Traffic**

When operating as a Voice Service Provider, Gizat 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.<sup>10</sup>

When operating as an Intermediate Provider, Gizat passes unaltered, any authenticated caller identification information for all calls it receives that use North American Numbering

Plan resources that pertain to the United States in the caller ID field. With respect to any unauthenticated calls it receives, Gizat is excused from authenticating such calls as Gizat participates cooperatively with the industry traceback consortium and responds fully and in a timely manner to all traceback requests it receives from the Commission, laws enforcement, and the industry traceback consortium.<sup>11</sup>

When operating as a Gateway Provider, Gizat authenticates caller identification information for all calls it receives that use North American Numbering Plan resources that pertain to the United States 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.<sup>11</sup>

---

<sup>10</sup> 47 C.F.R. § 64.6301(a).

<sup>11</sup> 47 C.F.R. § 64.6302(b) and (c).

## **7. Responding to Commission, Law Enforcement and ITG Traceback Requests**

Gizat is committed to ensuring that its 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. § 64.6305(b)(2) and 47 C.F.R. § 64.1200(n)(1)(ii), Gizat will respond to all traceback requests from the Commission, law enforcement, and the Industry Traceback Consortium ("ITG") within-24 hours<sup>12</sup> and will cooperate with such entities in investigating and stopping any illegal robocallers that attempt to use the network to carry or process calls. As part of this commitment, Gizat will take the necessary 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.<sup>13</sup> Gizat works closely with ITG and typically responds within one hour to ITG traceback requests.

## **8. Designating an Employee Responsible for Addressing Robocall Mitigation-Related Issues**

To further ensure GIZAT's network is not utilized for the origination, termination, or routing of unwanted and illegal robocalls, Gizat provides the following name, title, department, business address, telephone number, and email address of the individual within Gizat that leads Gizat'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:               | Ohad Harlev                                                          |
| Contact Title:              | Director                                                             |
| Contact City:               | Closter                                                              |
| Contact State and Zip Code: | NJ                                                                   |
| Contact Telephone Number:   | 5702510227                                                           |
| Contact Email:              | <a href="mailto:Support@gizatglobal.com">Support@gizatglobal.com</a> |

## **9. Updating the RMD Submission and RMP**

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

---

<sup>12</sup> This 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 FCC 22-37, at n.211

<sup>13</sup> See 47 C.F.R. § 64.1200(n)(2), (3) & (5).