

IDT TELECOM, INC. & AFFILIATES¹

Robocall Mitigation Program

February 2026 Version

¹ IDT America, Corp.; IDT Brasil Telecomunicações Ltda; IDT Corporation; IDT Corporation de Argentina S.A; IDT Domestic Telecom, Inc.; IDT Telecom México, S. de R.L. de C.V.; Net2Phone 2.0 America, Inc.; Net2Phone Cable Telephony, LLC; Net2Phone Chile SpA; Net2Phone Global Services, LLC; Net2Phone Peru S.A.C.; Versature Communications Corp.; IDT; IDT Enterprise; IDT Global Ltd; IDT Telecom Asia Pacific Limited; N2P; and Net2Phone.

Table of Contents

I.	Robocall Mitigation Program Introduction	1
A.	Company Summary	1
B.	Filing of RMP and Implementation of STIR/SHAKEN.....	1
II.	Robocall Mitigation Program	2
1.	Implementing Knowing Your Customer Protocols	3
2.	Requiring Contractual Provisions to Mitigate Illegal Robocalls.....	3
3.	Only Accepting Traffic from Providers in the RMD	4
4.	Blocking Calls on a Do-Not-Originate List	4
5.	Analyzing and Monitoring Network Traffic Routing Through IDT's Network ...	4
6.	Ensuring Foreign Providers Are Not Using IDT to Carry or Process High- Volume Illegal Traffic onto the U.S. Network.....	5
7.	Authenticating Voice Traffic	5
8.	Responding to Commission, Law Enforcement and ITG Traceback Requests	5
9.	Designating an Employee Responsible for Addressing Robocall Mitigation- Related Issues	6
10.	Updating IDT's RMD Submission and RMP	6

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 IDT Telecom, Inc. (“IDT Telecom”) and its affiliates² (both IDT Telecom and Affiliates are collectively referred to herein as, “IDT”) have established to prevent unlawful robocalls from originating on, terminating to, or routing through IDT’s voice networks 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

IDT Telecom and its Affiliates are subsidiaries of IDT Corporation, a Delaware corporation. Consistent with the FCC’s Robocall Mitigation Database (“RMD”) filing instructions,³ the Affiliates of IDT Telecom are also covered under this RMP and IDT Telecom has included the FCC Registration Numbers for all of these entities, where applicable, in its RMD filing, which are also listed in Exhibit A to this RMP.

IDT Corporation is a global provider of financial technology, or fintech, cloud communications and traditional communications services. Its consumer businesses make it easier for families to connect, support and share across international borders. With its commercial offerings, IDT Corporation enables businesses to transact and communicate with their customers with enhanced intelligence and insight. As indicated above, depending on the services provided, IDT Telecom and its Affiliates may serve as Voice Service Providers, Intermediate Providers, and/or Gateway Providers.

B. Filing of RMP and Implementation of STIR/SHAKEN

IDT has fully implemented STIR/SHAKEN and on June 29, 2021, 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). In accordance with the RMD 12/2022 Filing Instructions, FCC Rule 47 C.F.R. § 64.6305(b) and because IDT is a “Combined Gateway and Voice Service Provider” under these instructions, IDT has certified that IDT has “fully implemented the STIR/SHAKEN authentication framework across its entire network and all

² IDT America, Corp.; IDT Brasil Telecomunicações Ltda; IDT Corporation; IDT Corporation de Argentina S.A; IDT Domestic Telecom, Inc.; IDT Telecom México, S. de R.L. de C.V.; Net2Phone 2.0 America, Inc.; Net2Phone Cable Telephony, LLC; Net2Phone Chile SpA; Net2Phone Global Services, LLC; Net2Phone Peru S.A.C.; Versature Communications Corp.; IDT; IDT Enterprise; IDT Global Ltd; IDT Telecom Asia Pacific Limited; N2P; and Net2Phone (collectively, “Affiliates”).

³ 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>.

calls it carries or processes are compliant with FCC Rule, 47 C.F.R. § 64.6302(b).”⁴ In addition, IDT 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.”⁵

II. Robocall Mitigation Program

This RMP applies to IDT’s calling platforms and provides information on IDT’s policies and procedures on the following topics that are discussed in turn below which “details the specific reasonable steps [IDT] 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) Only Accepting Traffic from Providers in the RMD
- (4) Blocking Calls on a Do-Not-Originate List
- (5) Analyzing and Monitoring Network Traffic Routing Through IDT’s Network
- (6) Ensuring Foreign Providers Are Not Using IDT to Carry or Process High-Volume Illegal Traffic onto the U.S. Network
- (7) Authenticating Voice Traffic
- (8) Responding to Commission, Law Enforcement and ITG Traceback Requests
- (9) Designating an Employee Responsible for Addressing Robocall Mitigation-Related Issues
- (10) Updating IDT’s RMD Submission and RMP

⁴ 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”).

⁵ 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. 1⁶ and 47 C.F.R. § 64.1200(n)(3), IDT 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."⁷ In so doing, IDT 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."⁸

In this regard, IDT has implemented appropriate Know Your Customer ("KYC") protocols when onboarding new or renewing customers. As part of its KYC protocols, IDT requires any customer to provide sufficient information to ensure its legitimacy. Among other things, IDT 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, IDT 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.⁹

2. Requiring Contractual Provisions to Mitigate Illegal Robocalls

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

IDT's contracts include terms that forbid the customer from using IDT's 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. IDT's contract terms provide that if any calls originated or otherwise transmitted by the customer to IDT violate the TCPA, the TRACED Act, or the rules promulgated under these statutes, then IDT may, at its sole discretion, suspend or terminate the customer's service immediately, among other remedies.

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)(3).

⁹ See 47 C.F.R. § 64.6305(e)(1)-(3).

3. Only Accepting Traffic from Providers in the RMD

Accepting traffic from domestic Voice Service Providers. In accordance with 47 C.F.R § 64.6305(e)(1), IDT 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. If IDT receives notice that a provider has been delisted, it takes prompt action to stop receiving prohibited traffic.

Accepting traffic from Foreign Voice Service Providers and Foreign Intermediate Providers. In accordance with 47 C.F.R § 64.6305(e)(2), beginning 90 days after the deadline for filing certifications pursuant to 47 C.F.R § 64.6305(d) (which is April 11, 2023), IDT accepts calls directly from a Foreign Voice Service Provider or Foreign Intermediate Provider that uses North American Numbering Plan resources that pertain to the United States in the caller ID field to send voice traffic to residential or business subscribers in the United States, only if that foreign provider's filing appears in the RMD and that filing has not been de-listed pursuant to an enforcement action. If IDT receives notice that a provider has been delisted, it takes prompt action to stop receiving prohibited traffic.

Accepting traffic from Gateway Providers. In accordance with 47 C.F.R § 64.6305(e)(3), beginning 90 days after the deadline for filing certifications pursuant to 47 C.F.R § 64.6305(d) (which is April 11, 2023), IDT accepts calls directly from a Gateway Provider only if that Gateway Provider's filing (a) appears in the RMD showing that the Gateway Provider has affirmatively submitted its filing and RMP, and (b) has not been de-listed pursuant to an enforcement action. If IDT receives notice that a provider has been delisted, it takes prompt action to stop receiving prohibited traffic.

4. 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), IDT 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. IDT has protocols in place to detect DNO calls and blocks calls that are determined to originate from a DNO number.

5. Analyzing and Monitoring Network Traffic Routing Through IDT’s Network

Upon receiving call traffic, IDT also analyzes and monitors the call traffic that originates on, terminates to, or routes through IDT’s voice network. Consistent with Principal No. 5 of the FCC’s Caller ID Authentication Best Practices, IDT monitors the voice traffic patterns on a twenty-four (24) hour basis to identify behaviors that are consistent with illegal robocalling.

In this regard, IDT 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 IDT discovers call patterns that are consistent with illegal robocalling, IDT, 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.

6. Ensuring Foreign Providers Are Not Using IDT 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 IDT serves as a Gateway Provider for voice traffic that is routing through its network, IDT takes reasonable and effective steps discussed under Section 5, above, to ensure that any Foreign Voice Service Provider or Foreign Intermediate Provider from which IDT directly receives traffic is not using IDT, 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, IDT 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.

7. Authenticating Voice Traffic

When operating as a Voice Service Provider, IDT 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.¹⁰

When operating as a Gateway or Intermediate Provider, IDT 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.¹¹

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

IDT 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

¹⁰ 47 C.F.R. § 64.6301(a).

¹¹ 47 C.F.R. § 64.6302(b) and (c).

regulations 47 C.F.R. § 64.6305(b)(2) and 47 C.F.R. § 64.1200(n)(1)(ii), IDT will respond to all traceback requests from the Commission, law enforcement, and the Industry Traceback Consortium (“ITG”) within-24 hours¹² and will cooperate with such entities in investigating and stopping any illegal robocallers that attempt to use IDT’s network to carry or process calls. As part of this commitment, IDT 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.¹³ IDT works closely with ITG and typically responds within one hour to ITG traceback requests.

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

To further ensure IDT’s network is not utilized for the origination, termination, or routing of unwanted and illegal robocalls, IDT provides the following name, title, department, business address, telephone number, and email address of the individual within IDT that leads IDT’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:	Anthony Davidson
Contact Title:	EVP – Carrier Operations
Contact City:	Newark
Contact State and Zip Code:	New Jersey 07102
Contact Telephone Number:	(973) 438-4170
Contact Email:	Anthony.Davidson@idt.net

10. Updating IDT’s RMD Submission and RMP

Consistent with FCC Regulations, 47 C.F.R. § 64.6305(c)(5) & (d)(5), IDT 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.

¹² 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.

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

Exhibit A

<u>Company Name or Trade Name</u>	<u>FRN</u>
IDT America, Corp.	<u>0010522274</u>
IDT Brasil Telecomunicações Ltda	<u>0031068612</u>
IDT Corporation	<u>0006255251</u>
IDT Corporation de Argentina S.A.	<u>0031068588</u>
IDT Domestic Telecom, Inc.	<u>0010522381</u>
IDT Telecom, Inc.	<u>0010522506</u>
IDT Telecom México, S. de R.L. de C.V.	<u>0031069073</u>
Net2Phone 2.0 America, Inc.	<u>0031672017</u>
Net2Phone Cable Telephony, LLC	<u>0015288137</u>
Net2Phone Chile SpA	<u>0031068752</u>
Net2Phone Global Services, LLC	<u>0015288111</u>
Net2Phone Peru S.A.C.	<u>0031069115</u>
Versature Communications Corp.	<u>0031068729</u>
IDT	
IDT Enterprise	
IDT Global Ltd	
IDT Telecom Asia Pacific Limited	
N2P	
Net2Phone	

ADDENDUM TO ROBOCALL MITIGATION PLAN

IDT Telecom, Inc. and its affiliates, collectively (“IDT Telecom”), hereby provides this Addendum to Robocall Mitigation Plan (“Addendum”) to IDT Telecom’s Robocall Mitigation Plan “RMP”¹⁴ in accordance with the obligations set forth in *In the Matter of Call Authentication Trust Anchor, Sixth Report and Order and Notice of Proposed Rulemaking*, WC Docket No. 17-97 (March 17, 2023) ¶¶ 36-52 (“*Sixth R&O*”). The Addendum shall heretofore be incorporated within and be a part of IDT Telecom’s RMP.

In the *Sixth R&O*, the Commission stated, “First, to increase transparency for the industry and regulators and better facilitate our evaluation of the mitigation plans detailed in the Robocall Mitigation Database, we require providers to submit additional information to indicate the role or roles they are playing in the call chain.”¹⁵ Accordingly, IDT Telecom hereby states that for each call it handles that is subject to the Commission’s STIR/SHAKEN rules, IDT may be one of the following:

- (1) a voice service provider with a STIR/SHAKEN implementation obligation serving end-users;
- (2) a voice service provider with a STIR/SHAKEN obligation acting as a wholesale provider originating calls;
- (3) a non-gateway intermediate provider with a STIR/SHAKEN obligation; and
- (4) a gateway provider with a STIR/SHAKEN obligation.

In the *Sixth R&O*, the Commission stated, “Second ... providers with a current Robocall Mitigation Database filing obligation must state in their mitigation plan whether a STIR/SHAKEN extension applies.”¹⁶ IDT has implemented its STIR/SHAKEN obligations and has filed its initial RMP and herein we file the additional information required by the *Sixth R&O*. Accordingly, IDT hereby states that a STIR/SHAKEN extension is neither requested nor needed and a request for an extension does not apply.

In the *Sixth R&O*, the Commission stated, “Third, we require new and existing filers to certify that they have not been prohibited from filing in the Robocall Mitigation Database pursuant to a law enforcement action, including the new enforcement requirements adopted herein.”¹⁷

Accordingly, IDT Telecom hereby states that it has not been prohibited from filing in the Robocall Mitigation Database pursuant to a law enforcement action, including the new enforcement requirements adopted herein. Moreover, IDT Telecom certifies that it has not been barred from filing in the Robocall Mitigation Database by such an enforcement action, including,

¹⁴If any statements or other information in the Addendum are in any way inconsistent with statements in the original RMP, the statements in the Addendum shall supersede the previously drafted statements.

¹⁵ *Sixth R&O* at ¶ 44.

¹⁶ *Id.* at ¶ 45.

¹⁷ *Id.* at ¶ 46.

but not limited to, instances in which a provider has been removed from the Robocall Mitigation Database and has been precluded from refiling unless and until certain deficiencies have been cured and those in which a provider's authorization to file has been revoked due to continued violations of the Commission's robocall mitigation rules.

In the *Sixth R&O*, the Commission stated, "Fourth, we require all providers to: (1) state whether, at any time in the prior two years, the filing entity (and/or any entity for which the filing entity shares common ownership, management, directors, or control) has 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 the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description; and, if so (2) provide a description of any such action or investigation, including all law enforcement or regulatory agencies involved, the date that any action or investigation was commenced, the current status of the action or investigation, a summary of the findings of wrongdoing made in connection with the action or investigation, and whether any final determinations have been issued."¹⁸

However, the Commission narrowed the possible scope of the reporting obligation when it stated, "We limit this reporting requirement to formal actions and investigations that have been commenced or issued pursuant to a written notice or other instrument containing findings by the law enforcement or regulatory agency that the filing entity has or is suspected of the illegal activities itemized above, including, but not limited to, notices of apparent liability, forfeiture orders, state or federal civil lawsuits or criminal indictments, and inquiries from law enforcement or regulatory agencies or investigations that do not include findings of actual or suspected wrongdoing. Thus, for example, traceback requests, Enforcement Bureau letters of inquiry or subpoenas, or investigative demand letters or subpoenas issued by regulatory agencies or law enforcement would not trigger this obligation because they are not accompanied by findings of actual or suspected wrongdoing. We find that inquiries or investigations that do not contain findings of actual or suspected wrongdoing by the law enforcement or regulatory agency would be of limited value to the Commission in evaluating the certifications and robocall mitigation plans submitted to the Robocall Mitigation Database."¹⁹

Accordingly, IDT Telecom hereby states that it 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 the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description. While IDT Telecom has received some or all of the requests listed by the Commission (e.g., inquiries from law enforcement or regulatory agencies or investigations such as traceback requests, Enforcement Bureau letters of inquiry or subpoenas, or investigative demand letters or subpoenas issued by regulatory agencies or law enforcement), these requests did not include findings of actual or suspected wrongdoing. As a result, they do not trigger the aforementioned reporting obligation

¹⁸ *Id.* at ¶ 47.

¹⁹ *Id.* (Footnotes omitted.)

because they were not accompanied by findings of actual or suspected wrongdoing.

The *Sixth R&O* also requires filers to “submit their OCN if they have one.”²⁰ IDT Telecom subsidiary IDT America, Corp. holds two OCNs: 367B and 363A.

Additionally, in the *Sixth R&O*, the Commission stated, “Specifically, as part of their obligation to ‘describe with particularity’ their robocall mitigation techniques, (1) voice service providers must describe how they are meeting their existing obligation to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls; (2) non-gateway intermediate providers and voice service providers must, like gateway providers, describe any “know-your-upstream provider” procedures in place designed to mitigate illegal robocalls; and (3) all providers must describe any call analytics systems they use to identify and block illegal traffic, including whether they use a third-party vendor or vendors and the name of the vendor(s).

As stated earlier in this Addendum, IDT Telecom is, for certain calls, a voice service provider with a STIR/SHAKEN implementation obligation serving end-users as well as a wholesale provider originating calls. In Section II of its previously filed RMP, IDT describes in considerable detail how it is meeting its obligation to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls. That Section is incorporated by reference.

IDT has also, over time, developed contract language to reflect its obligations under current and developing STIR/SHAKEN rules. Below, we have included sample contract language that IDT Telecom has developed contemporaneously with the filing of this Addendum. It is not the position of IDT Telecom that this language is in all previously signed contracts. Rather, this language is consistent with language presented to new customers, to the degree applicable.

X. Prohibited Uses. Notwithstanding anything to the contrary contained herein, Company reserves the right, in its sole discretion, to immediately and without notice terminate the Service to you (and generally) for any use of the Service or any other action that causes a disruption in Company’s network integrity, or directly or indirectly threatens or compromises the security of Company, its vendors, or the Service, or that otherwise violates this Section 6. You agree that you will use the Service for your own internal use only, and will not resell, transfer or charge for the Service or Equipment without the express written permission of the Company. Permitted use of the Service does not include certain activities including, but not limited to autodialing, robocalling, transmitting any material that contains viruses, time bombs, trojan horses, worms, malware, spyware, or any other programs that may be harmful or dangerous, spoofing, continuous or extensive call forwarding, continuous connectivity, fax broadcast, fax blasting, polling, transmitting any material that may infringe, misappropriate, or otherwise violate the foreign or domestic intellectual property rights or other rights of third parties, telemarketing (including without limitation charitable or political solicitation, junk faxing, fax spamming, calling/faxing any

²⁰ *Id.* at ¶ 48.

person through the use of distribution lists or otherwise who has not given specific permission to be included in such a process) or any other activity that would be inconsistent with reasonable business usage. These prohibitions shall not be construed to prevent autodialing, robocalling, and/or telemarketing by users of the CCaaS Services in accordance with the terms thereof. You shall not transmit through the Service any unlawful, harassing, defamatory, abusive, threatening, harmful, vulgar, obscene, indecent, or otherwise objectionable communications or material of any kind or nature. You further agree not to transmit any material that encourages conduct that could constitute a criminal offense, violate the intellectual property rights of others, give rise to civil or criminal liability or otherwise violate any applicable local, state, national or international statute, regulation, or other law. You agree that you will, at all times, comply with all applicable law. Applicable law includes, as applicable, the Telephone Consumer Protection Act and the Telemarketing Sales Rule, the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (“TRACED Act”), the Truth in Caller ID Act, the Junk Fax Act, the CAN-SPAM Act, similar state laws, state laws regarding privacy and data subject rights, and the requirements of the Payment Card Industry Data Security Standard (“PCI DSS”). You further agree that you will not use a fax line to place voice calls. You agree that the Services are not intended for use with alarm systems or elevator telephone systems.

Additional Restrictions on USA Traffic:

You warrant and represent that: (1) you are not a provider of ‘voice service’ as defined by 47 CFR Section 64.6300(n); (2) you are not a ‘foreign voice service provider,’ as defined by 47 CFR Section 64.6300(c); (3) you are not an Intermediate Service Provider (ISP), as that term is defined by 47 CFR Section 64.6300(g); (4) all traffic sent by you to Company shall be originated in the conduct of your legitimate business, on your equipment, and using originating numbers that you have the legal right to use; and (5) neither you nor any of your affiliates or principals have ever been the recipient of a cease and desist, mandatory blocking, or similar order from the FCC, FTC, or other federal or state agency with respect to the transmission of voice or fax traffic. You will not send to Company traffic as a voice service provider, a foreign voice service provider or intermediate service provider (meaning, traffic originated by third parties and transited by you).

You further warrant and represent that when placing telemarketing calls to end-users located in the United States:

- You will not make or transmit telemarketing calls using an artificial or prerecorded voice to *residential* telephones without prior express consent.
- You will not make or transmit *any* non-emergency call using an automatic telephone dialing system (“autodialer”) or an artificial or prerecorded voice to a *wireless* telephone number unless you have received proper consent.
- You will not initiate or transmit a telephone solicitation to a residential telephone subscriber who has registered his or her telephone number on the national “Do-Not-Call” registry.

- You acknowledge that telemarketing calls can only be made between the hours of 8 a.m. and 9 p.m. (local time at the called party's location).
- You will comply with limits on "abandoned calls" and employ other consumer-friendly practices when using automated telephone-dialing equipment, noting that a telemarketer must abandon no more than 3 percent of calls answered by a person and must deliver a prerecorded identification message when abandoning a call. Two or more telephone lines of a multi-line business are not to be called simultaneously. Telemarketers must not disconnect an unanswered telemarketing call prior to at least 15 seconds or four rings.
- You acknowledge that if you use an auto dialer to sell services, then you must maintain records documenting compliance with call abandonment rules.
- Numbers in the CLI presentation field will allow a recipient of such calls to call back to the presented number and have it be reasonably answered.
 - All prerecorded messages, whether delivered by automated dialing equipment or not, must identify the name of the entity responsible for initiating the call, along with the telephone number of that entity that can be used during normal business hours to ask not to be called again.
 - You must transmit caller ID information, when available, and must refrain from blocking any such transmission(s) to the end user. You may not alter the caller ID information with intent to deceive the recipient or disguise the origin of the call.

If any calls originated or otherwise transmitted by you to Company violate the terms of applicable law, then Company may, in its sole discretion, in addition to the remedies contained in these Terms of Service, suspend or terminate the Services immediately and freeze some and/or all prepaid monies remitted by you to Company until such time that Company, at its sole discretion, has determined it shall not be subject to any penalties, fines and/or "voluntary contributions" by the Federal Communications Commission and/or other third parties who have or may obtain a legal right of payment. Should the Company be subject to any penalties, fines and/or "voluntary contributions," Company may use any frozen payments as partial payment to the third party(ies) and Company may seek payment from you for any additional, required payments. You will cooperate with and promptly provide information requested in connection with any traceback requests.

Any use found to be inconsistent with any of the restrictions set forth herein may result in the immediate termination of the Service. You also understand that IDT Telecom may immediately suspend or terminate Your right to use the Service, without liability of any kind, if (a) in IDT Telecom's sole discretion, Your use of the Service exceeds what would be expected of normal business use, or (b) Your use of the Messaging Services is not typical of human message origination and termination or if there is an abnormal imbalance of inbound and outbound messaging. IDT Telecom reserves the right, in its sole discretion, to block access to certain high cost/premium locations. Please contact IDT Telecom Customer Support for more information.

Also, as stated earlier in this Addendum, IDT Telecom is, for certain calls, a voice service provider; a non-gateway intermediate provider and/or a non-gateway intermediate provider. As a result, IDT has “know-your-upstream provider” procedures in place designed to mitigate illegal robocalls. These procedures are as follows.

Consistent with the FCC’s Caller ID Authentication Best Practices No. 1²¹ and 47 C.F.R. § 64.1200(n)(3), IDT 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.”²² In so doing, IDT 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.”²³

In this regard, IDT has implemented appropriate Know Your Customer (“KYC”) protocols when onboarding new or renewing customers. As part of its KYC protocols, IDT requires any customer to provide sufficient information to ensure its legitimacy. Among other things, IDT 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, the industry in which the customer participates and nature of the customer’s business as well as the customer’s traceback history. If the company is a Voice Service Provider, Foreign Voice Service Provider, Intermediate Provider, and/or Gateway Provider, IDT 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.²⁴

Finally, In the *Sixth R&O*, the Commission demands that “all providers must describe any call analytics systems they use to identify and block illegal traffic, including whether they use a third-party vendor or vendors and the name of the vendor(s).” Therefore, as requested by the Commission, IDT Telecom hereby describes how it is meeting its afore-stated obligations. IDT Telecom uses internally developed electronic as well as manual customer analytics tools designed to monitor our traffic for suspicious patterns. IDT considers these tools confidential and proprietary but will make them available to the Commission upon request. What makes a pattern “suspicious” is the result of multiple factors, which may (and likely will) vary based on numerous considerations including, but not limited to: commercial history with IDT of entity transmitting traffic to IDT Telecom; terminating location of traffic; length of calls; originating ANIs of traffic; prior understanding of IDT Telecom regarding the traffic to be transported; country/region of originating calls; as well as other factors which may or may not be considered in all instances.

²¹ 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>.

²² *Id.*

²³ 47 C.F.R. § 64.1200(n)(3).

²⁴ *See*, 47 C.F.R. § 64.6305(e)(1)-(3).

Also, we subscribe to/use You Mail Protective Services; we compare ANIs against a Do Not Originate list provided by Somos, Inc. through their subsidiary, XConnect,²⁵ to block such traffic automatically and we block all numbers on the Industry Traceback Group Do Not Origin List. IDT Telecom is consistently reviewing and considering the implementation of additional DNO lists and we anticipate adding these Lists as warranted.

²⁵ <https://www.somos.com/insights/idt-global-selects-xconnect-tackle-robocalls-intelligent-dno-data> (Last viewed: July 6, 2023).