

Robocall Mitigation Plan

Dear Textdrip Customer and/or Vendor,

Textdrip, LLC is a wholesale VoIP termination provider, and an “Intermediate Provider” which means:

- 1) It must register with the FCC and obtain an FCC Registration Number (FRN),
- 2) Textdrip LLC **must register with the Robocall Mitigation Database and certify its level of STIR/Shaken implementation.**

Item number 2 above is TEXTDRIP’s newest obligation resulting from a national effort to reduce *illegal* robocall activity. TEXTDRIP is compliant with all of its obligations above. As part of TEXTDRIP’s compliance, with item number 2 above, **beginning on September 28, 2021**, TEXTDRIP along with all other **Intermediate Providers and Terminating Voice Service**

Providers will be prohibited from accepting traffic from voice service providers and intermediate providers who are not listed in the Robocall Mitigation Database.

This means that in order to comply with the new FCC Orders, STIR/SHAKEN caller ID authentication framework and TRACED Act, all of **TEXTDRIP’s customers and vendors must be registered in the Robocall Mitigation Database** unless, the customer is an end-user.

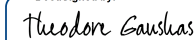
If the customer is an end-user, the Intermediate Provider or Voice Service Provider must participate in a TRACEBACK request and/or law enforcement efforts to identify illegal robocalls.

Additionally, Textdrip LLC (along with its customers and vendors) are required to implement a Robocall Mitigation Program. With the new FCC order, TEXTDRIP has edited its program and policies as follows: All TEXTDRIP Customers **MUST** be registered with the FCC Robocall Mitigation Database before September 1, 2021 otherwise, TEXTDRIP will no longer accept their traffic.

As a wholesale VoIP termination provider that specializes in legal, legitimate, wanted auto-dialer traffic, Textdrip LLC is committed to doing its part to eliminate illegal, fraudulent, and unwanted robocall traffic. To that end, we’ve included a document with this letter entitled; “Robocall Mitigation Plan” that outlines the requirements imposed on us as well as our customers and vendors in order for you to better understand those obligations.

Best Regards,

DocuSigned by:



Theodore Gaushas, COO

Phone: 1-248-259-0100

Email: compliance@textdrip.com

ROBOCALL MITIGATION OBLIGATIONS

Related to FCC Public Notice DA 21-454 (WC Docket No. 17-97)

This document is created by Textdrip LLC to help its customers and vendors navigate some of the new robocall mitigation obligations imposed by the US Congress and enforced by the FCC.

The main obligations covered in this document are related to the Robocall Mitigation Database, The STIR/SHAKEN caller ID authentication framework, and the TRACED Act. The entities affected by, and discussed in, this document are Voice Service Providers, Intermediate Providers, and Terminating Voice Service Providers.

NOTICE: This document is not intended to provide legal advice. It is strongly suggested that an attorney be consulted for definitive advice on these matters. AKA Management, Inc. is attempting to share the information it has found with regard to the subject matter above for educational purposes only, in an attempt to help mitigate illegal robocalls.

Overview:

On 12/30/2020, the FCC issued an order that requires ALL voice service providers to "Take 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."

The FCC "gives voice service providers the flexibility to decide the specific contours of an effective robocall mitigation program that best suits the needs of their networks and customers." When assessing the robocall environment, it is important to make a distinction between legal and illegal robocalls. The Telephone Consumer Protection Act ("TCPA"), regulates certain calls made using an "automatic telephone dialing system" or an "artificial or prerecorded voice" to *residential and cellular* phones, if a *consumer* has not consented to receive such calls. If a *consumer has consented* to receive a robocall, or the call is destined to a *business*, who's phone number is often the same as a consumer's personal number, the *call is NOT illegal*. Legitimate businesses and organizations regularly utilize legal robocalls to provide consumers with critical and time-sensitive information, such as fraud alerts, school closures, prescription notices, and appointment reminders.

In contrast however, illegal robocalls can range from unlawful solicitations for products and services, to outright fraudulent and criminal activity. Additionally, Caller ID spoofing, calling consumers without prior written permission or business relationship, not providing consumers with an option to opt-out of receiving calls, calling numbers on the Do-Not-Call registry, calling residences before 8 AM or after 8 PM, and failing to identify themselves when making calls.

For clarification, there are plenty of legitimate, legal and desired robocalls by both businesses and consumers. There is a common misconception that all robocalls are illegal, fraudulent, unwanted or malicious and that is just not the case. As with all industries and technology, there are those who operate illegally and it is all of our job to eliminate bad actors from the landscape wherever possible.

Voice Service and Intermediate Provider Obligations:

Here are the key dates and obligations that Intermediate Providers and Voice Service Providers must know.

- **June 30, 2021:** Deadline for Voice Service Providers to submit required information into the Robocall Mitigation Database (https://fccprod.servicenowservices.com/rmd?id=rmd_welcome)
- **June 30, 2021:** Deadline for Voice Service Providers to draft and implement a Robocall Mitigation Program.
- **September 28, 2021:** Deadline for Intermediate Providers and Terminating Voice Service Providers to Cease accepting traffic from Voice Service Providers not listed in the Robocall Mitigation Database.

Reference Documents:

The following notices and information is published by the FCC specifying its rulings and instructions.

- **FCC Public Notice DA 21-454 (WC Docket No. 17-97) WIRELINE COMPETITION BUREAU ANNOUNCES OPENING OF ROBOCALL MITIGATION DATABASE AND PROVIDES FILING INSTRUCTIONS AND DEADLINES** <https://docs.fcc.gov/public/attachments/DA-21-454A1.pdf>
- **FCC Public Notice DA 20-1526 (WC Docket Nos. 17097 and 20-234) WIRELINE COMPETITION BUREAU ISSUES CALLER ID AUTHENTICATION BEST PRACTICES** https://docs.fcc.gov/public/attachments/DA-20-1526A1_Rcd.pdf
- **Robocall Mitigation Database External Filing Instructions (Version: April 2021)** <https://www.fcc.gov/sites/default/files/rmd-instructions.pdf>

Legal Citations:

The United States laws that apply here are located in the Code of Federal Regulations (CFR) Title 47 – Telecommunication – Chapter I – Federal Communications Commission – Subchapter B – Common Carrier Services – Part 64 – Miscellaneous Rules Relating To Common Carriers – Subpart HH – Caller ID Authentication

47 CFR § 64.6300 - Definitions

47 CFR § 64.6301 - Caller ID authentication

47 CFR § 64.6302 - Caller ID authentication by intermediate providers

47 CFR § 64.6303 - Caller ID authentication in non-IP networks

47 CFR § 64.6304 - Extension of implementation deadline

47 CFR § 64.6305 - Robocall mitigation and certification

All of the above regulations, the most important one is the last one (47 CFR § 64.6305 - Robocall mitigation and certification) because all Voice Service, and Intermediate Providers have an obligation to register and certify their level of STIR/SHAKEN implementation.

Here is a link to the Robocall Mitigation Database URL: https://fccprod.servicenowservices.com/rmd?id=rmd_welcome. If you have an account, log in and if not, click Create an Account. To create an account, you'll first need to obtain a FCC Registration Number (FRN). You'll be able to do so when you click the "create account" button. Don't worry, its not hard and anyone can do so regardless of your geographic location or if you even have a formal company.

There are other items to fill out and here is a link for instructions on how to do so. But the key part of the registration is certifying your level of STIR/SHAKEN implementation. Here are the options you'll be able to choose from once you are in:

Certification (Choose one)

Option 1: Complete STIR/SHAKEN Implementation. The filer certifies that all voice traffic that originates on its network is authenticated with STIR/SHAKEN, consistent with 47 CFR § 64.6301(a).

Option 2: Partial STIR/SHAKEN Implementation – Performing Robocall Mitigation. The filer certifies that it commits to respond 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, and that some of the voice traffic that originates on its network is authenticated with STIR/SHAKEN, and the remainder of the voice traffic that originates on its network is subject to a robocall mitigation program. The filer also certifies that the attached searchable PDF details the specific reasonable steps it has taken to avoid originating illegal robocall traffic as part of its robocall mitigation program, and, if applicable, the type of extension or extensions it received under 47 CFR § 64.6304.

Option 3: No STIR/SHAKEN Implementation – Performing Robocall Mitigation. The filer certifies that it commits to respond 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, and that none of the voice traffic that originates on its network is authenticated with STIR/SHAKEN, and that all of the voice traffic that originates on its network is subject to a robocall mitigation program. The filer also certifies that the attached searchable PDF details the specific reasonable steps it has taken to avoid originating illegal robocall traffic as part of its robocall mitigation program, and, if applicable, the type of extension or extensions it received under 47 CFR § 64.6304.

Recommended Option:

You'll need to select the correct option that applies to you. However, unless you are technically able to verify the caller identification information using an SPC Token (see definition here) you will need to select Option 3. Selecting Option 3 means:

- a. You'll need to be prepared to implement a Robocall Mitigation Plan and
- b. You'll need to cooperate with the Industry Traceback Consortium to assist in finding the origin of suspected unlawful robocalls.

How to Structure an Effective Robocall Mitigation Plan

Not all auto-dialed traffic is illegal. Providers who process auto-dialed traffic should develop Robocall Mitigation Plan (RMP). Key elements of an RMP for auto-dialed traffic should include:

1. Cooperation in Contracts: Make sure your contract (Terms of Service and/or Acceptable Use Policy) is clear about the kind of traffic you will (and will not) accept from your customers. Tell them that if they do not follow the rules, they will be subject to prompt termination. If they are found sending calls you believe are illegal, they will forfeit confidentiality and their information will be shared with enforcers and industry partners.
2. Know Your Customer: Voice service providers should confirm the identity of new commercial customers by collecting information such as physical business location, contact person(s), state or country of incorporation, federal tax ID (if applicable), and the nature of customer's business. Vet each customer thoroughly. Make sure any suspicions are allayed before turning on service. Do not give anonymous test accounts to auto-dialers.
3. Quick Action: Have a plan that allows you to act promptly and decisively on anything suspicious detected by your monitoring. If you get a traceback notice for an illegal robocall, do not leave issues unresolved; insist on specific, deterministic explanations with explicit corrective actions. Fraud callers and customers with sloppy controls cannot be rewarded with on-going forgiveness.
4. Published Policies: Make sure you have a record of notifying your customer(s) of your policies regarding illegal robocalls and your intolerance of them.
5. Be especially suspicious of foreign sources sending auto-dialed traffic using USA +1 telephone numbers. There are only a very few legitimate scenarios for this; often, the traffic is completely fraudulent.
6. Robocall Mitigation Database: Ensure that your customer(s) have registered with the Robocall Mitigation Database.
7. Call Blocking: Ensure your call routing platform has the ability to block calls destined to specified phone numbers
8. Cooperate with Investigative Bodies: Be ready to comply with traceback requests by law enforcement, the FCC, or the Industry Traceback Group, the official consortium designated to lead private traceback efforts. Companies should designate a single point of contact to handle traceback requests and coordinate with outside investigations.

Definitions:

These definitions are excerpts from the Code of Federal Regulations cited below.

Voice service. The term voice service:

1. Means any service that is interconnected with the public switched telephone network and that furnishes voice communications to an end user using resources from the North American Numbering Plan or any successor to the North American Numbering Plan adopted by the Commission under section 251(e)(1) of the Communications Act of 1934, as amended; and
2. Includes transmissions from a telephone facsimile machine, computer, or other device to a telephone facsimile machine.

Intermediate provider. The term intermediate provider means any entity that carries or processes traffic that traverses or will traverse the public switched telephone network (PSTN) at any point insofar as that entity neither originates nor terminates that traffic.

Interconnected VoIP Service provider is a provider of VoIP services that: 1) enable real-time, two-way voice communications; 2) require a broadband connection; 3) require IP-compatible customer equipment; and 4) permit subscribers to receive calls from and place calls to the Public Switched Telephone Network.

STIR/SHAKEN authentication framework. The term STIR/SHAKEN authentication framework means the secure telephone identity revisited and signature-based handling of asserted information using tokens standards.