

ONTIMETELECOM, INC.
ROBOCALL MITIGATION PLAN
MARCH 2025

I. Background

The Federal Communications Commission (“FCC” or “Commission”) requires that all voice service providers certify, by June 30, 2021, in the Commission’s [Robocall Mitigation Database](#) whether they have implemented STIR/SHAKEN or, if subject to an applicable extension, that they have documented and instituted a robocall-mitigation plan to help combat the origination of illegal robocalls on their networks.[1] The Commission has explained that a robocall-mitigation program is sufficient if the detailed practices in the plan can “reasonably be expected to significantly reduce the origination of illegal robocalls” and the voice service provider complies with the practices it describes in its filings.

OnTimeTelecom is dedicated to stopping illegal calls from originating on its network, and this document outlines OnTimeTelecom’s Robocall Mitigation plan.

II. Commitment to Traceback Cooperation

OnTimeTelecom commits to timely cooperating with and responding to Traceback requests from the FCC Enforcement Bureau, ITG (or any successor entity designated by the FCC), trace-forward investigations, and other valid law enforcement and government demands, subpoenas, and other valid legal processes. OnTimeTelecom will dedicate sufficient resources to provide prompt and complete responses to such requests. OnTimeTelecom will investigate suspicious activity found by its monitoring systems or reported to it by consumers or third parties and take appropriate action.

OnTimeTelecom has adopted the following additional internal procedures to carry out its commitment to cooperate with Traceback requests and to take appropriate remedial actions when warranted:

- Michael Freedman, OnTimeTelecom’s CTO and co-founder, has been designated the responsible officer and will coordinate the handling of all Traceback requests that are received.
 - David Batchelor is also a co-founder and the President of OnTimeTelecom. Mr. Freedman and Mr. Batchelor are the sole owners and principals of OnTimeTelecom.
- When a traceback request is received, OnTimeTelecom will email the customer a list of questions necessary to properly investigate the scope of the Traceback request and if the calls are legitimate or not.
- OnTimeTelecom will also promptly call the relevant customer to inform them of the Traceback request, and that OnTimeTelecom has sent the customer an email requesting specific information related to the investigation.

- **If the customer does not respond within 24 hours, OnTimeTelecom will suspend the account** – without limiting other actions OnTimeTelecom may take.
- OnTimeTelecom will separately perform an audit of the subject account, and suspend or terminate the account if deemed to be sending illegal content or calls in violation of OnTimeTelecom's Acceptable Use Policy ("AUP").
- OnTimeTelecom's goal is to comply with all Traceback requests within 24 hours if commercially reasonable, and sooner when practicable.

III. OnTimeTelecom's Know Your Customer ("KYC") Standards

OnTimeTelecom is a voice, text and email service provider that focuses its operations on the government, non-profit and business customer segment of the communications market. As part of its customer-onboarding process, OnTimeTelecom undertakes various commercially reasonable precautions to verify a given customer's identity as part of entering into a formal written agreement.

During the initial prospective-customer screening process, OnTimeTelecom collects the following customer-identifying information when possible:

- Customer entity or business name,
- Customer email,
- Customer physical address,
- Customer telephone numbers, and
- Contact person(s).

Once obtaining this information, OnTimeTelecom support and sales staff will attempt to personally contact all prospective customers during the enrollment process for further vetting, multiple times if necessary. OnTimeTelecom then requires the prospective customer to verify all caller IDs to be used through OnTimeTelecom's service through a verification process that entails OnTimeTelecom placing an outbound call with a pin code to each telephone number, which the prospective customer must then enter to verify the telephone number.

IV. OnTimeTelecom's Acceptable Use Policy

As part of its customer-onboarding process, all of OnTimeTelecom's customers contractually agree to various terms and conditions, including a commitment to comply with OnTimeTelecom's Acceptable Use Policy (AUP). Among other things, this AUP prohibits:

- Engaging in any unsolicited advertising, marketing or other activities, including any activities that violate anti-spam laws and regulations, including, but not limited to, the CAN-SPAM Act of 2003, the Telephone Consumer Protection Act, the Telemarketing and Consumer Fraud and Abuse Prevention Act, and the Do-Not-Call Implementation Act (or any similar or analogous anti-spam, data protection, or privacy statutes or regulations in any other jurisdiction);

- Using the Services in any manner that violates: industry standards; any third party policies including all of the applicable guidelines published by the CTIA, the Mobile Marketing Association, or any other accepted industry associations, carrier guidelines (or any similar or analogous industry standards, third party policies or requirements in any other jurisdiction);, or requirements that [OnTimeTelecom] may communicate to its Customers.
- Misleading others as to the identity of the sender of your messages or broadcasts, by creating a false identity, impersonating the identity of someone/something else or by providing contact details that do not belong to you; and
- Transmitting, associating or publishing any unlawful, racist, harassing, libelous, abusive, threatening, demeaning, immoral, harmful, vulgar, obscene, pornographic or otherwise objectionable material of any kind.

Customers must also affirmatively comply the following additional requirements:

- Identify yourself or your organization in your messages as required by any applicable law;
- Schedule the timing of your messages responsibly and adhere to any calling time restrictions that may be applicable to your messages; and
- Immediately honor any Do-Not-Call or opt-out requests that are communicated to you and use the internal Do Not Call lists to allow your call recipients to opt-out from future messages you send from your account. Keep monitoring this list to see who is opting out. It's located in the "My Account" section of your [OnTimeTelecom] account.

OnTimeTelecom's contracts with its customers stipulate that OnTimeTelecom is authorized to suspend and/or terminate all Services in the event of an AUP violation.

V. Telephone Number Authorization and STIR-SHAKEN Capabilities

OnTimeTelecom's service combines various enhanced information services with the outbound calling capabilities provided by underlying carriers. OnTimeTelecom is not subject to STIR/SHAKEN implementation requirements, as it lacks control over the network infrastructure necessary to implement STIR/SHAKEN. That said, OnTimeTelecom's understanding is that its underlying carriers are authenticating OnTimeTelecom's customers' traffic pursuant to STIR/SHAKEN. And as noted above, OnTimeTelecom's end users can only use telephone numbers which they have verified are assigned to them, such that OnTimeTelecom has a documented, verified relationship between the originating end user and their telephone number(s) used to originate their calls.

VI. Proactive Network Monitoring and Fraud Prevention

OnTimeTelecom has various monitoring, fraud prevention and reporting systems in place to analyze traffic on its network for potentially suspicious traffic patterns that are likely to be associated with illegal robocalls or other potentially unlawful usage. For example,

OnTimeTelecom disallows proxies, public VPNs, Tor, and similar services from using its Services by default. OnTimeTelecom also blocks prospective customer enrollment from countries associated with high levels of fraud, and further uses advanced credit card fraud prevention practices to stop transactions from occurring before outbound traffic can be initiated by customers. OnTimeTelecom also uses automated processes to detect patterns consistent with illegal robocalls before they are sent.

OnTimeTelecom also conducts retrospective analyses of customer calling patterns, including in part, by comparing customer caller IDs against the Federal Trade Commission's Do Not Call (DNC) Reported Calls Data. This entails a daily review of this consumer-complaint data set to discover whether any OnTimeTelecom customers were the subject of a consumer complaint and to take appropriate remedial action where warranted.

While OnTimeTelecom performs the steps above internally, it also uses the following third-party vendors as part of its overall approach to detecting bad actors and potential fraudulent activity to enhance its robocall mitigation efforts:

- **FingerprintJS** – Device fingerprinting to detect fraudulent users and identify repeat offenders.
- **IPQualityScore (IPQS)** – VPN detection, proxy detection, and risk scoring for incoming traffic.
- **MaxMind** – Geolocation and fraud risk analysis to identify and block high-risk signups and transactions.

Pursuant to FCC Rule 64.6305(d)(2)(ii), OnTimeTelecom states that the foregoing analytics services are the third-party services utilized by OnTimeTelecom.

VII. Additional Information Required By *Sixth Report and Order*

The FCC requires that all voice service providers certify, by February 26, 2024, in the Commission's RMD whether they have implemented the STIR/SHAKEN authentication framework, and that all of the calls that it originates, carries or processes are subject to a robocall mitigation program consistent with the Commission's rules.¹ The provider's mitigation plan "shall include reasonable steps to avoid originating illegal robocall traffic and shall include 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

¹ See <https://docs.fcc.gov/public/attachments/DA-24-73A1.pdf> (WCB Jan. 25, 2024 Public Notice).

investigating and stopping any illegal robocallers that use its service to originate calls.” 47 C.F.R. § 64.6305(a)(2).²

OnTimeTelecom notes that, by design, its services are provisioned to significantly curtail end users’ ability to spoof their telephone numbers. OnTimeTelecom’s end users can only use caller IDs that they have verified, through the process described above, as their outbound caller ID, such that, absent some hacking event, which would violate OnTimeTelecom’s AUP, OnTimeTelecom’s end users cannot manipulate their caller ID. Thus, by design, OnTimeTelecom’s end users are prevented from using OnTimeTelecom’s services to violate 47 U.S.C. § 227(e).

The FCC’s rules contemplate that the provider’s plan should describe how it “complies with its obligation to know its customers pursuant to § 64.1200(n)(4), any procedures in place to know its upstream providers, and the analytics system(s) it uses to identify and block illegal traffic, including whether it uses any third-party analytics vendor(s) and the name(s) of such vendor(s).” 47 C.F.R. § 64.6305(d)(1)(ii). The Commission has acknowledged, however, that, “we do not currently require [] providers other than gateway providers to engage in ‘know-your-upstream-provider’ procedures, [but] if they have put such procedures in place, they must be documented in their robocall mitigation plan,” and that “we do not specifically require providers to use call analytics.” *Sixth Caller ID Authentication Report and Order* ¶ 40 & n.155-56. That said, OnTimeTelecom directs the Commission to its KYC standards detailed above.

² The TRACED Act defines “robocall violation” as “a violation of subsection (b) or (e) of section 227 of the Communications Act of 1934.” TRACED Act § 11(d), Pub. L. No. 116-105, 133 Stat. 3274 (2019); *id.* at § 13(d)(f)(3) (defining a “suspected unlawful robocall” as a “call that the Commission or a voice service provider reasonably believes was made in violation of subsection (b) or (e) of section 227 of the Communications Act of 1934.” Thus, OnTimeTelecom’s training and mitigation efforts focus, consistent with the TRACED Act, on potentially unlawful calls that violate either (a) 47 U.S.C. § 227(b) (governing non-emergency calls initiated with a prerecorded or artificial voice or an automatic telephone dialing system, as that term has been interpreted by the Supreme Court in *Facebook, Inc. v. Duguid*, 592 U.S. 395 (2001)) or (b) 47 U.S.C. 227(e), or the Truth in Caller ID Act, which prohibits people from causing “any caller identification service to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value,” absent an applicable exemption.