

TELE-TOWN HALL, LLC
ROBOCALL MITIGATION PLAN
FEBRUARY 2024

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.

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

II. Commitment to Traceback Cooperation

Tele-Town Hall 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. Tele-Town Hall will dedicate sufficient resources to provide prompt and complete responses to such requests. Tele-Town Hall will investigate suspicious activity found by its monitoring systems or reported to it by consumers or third parties and take appropriate action.

Tele-Town Hall 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:

- Christopher Elizondo Tele-Town Hall’s Chief Customer Officer, has been designated the responsible officer and will coordinate the handling of all Traceback requests that are received.
- When a traceback request is received, Tele-Town Hall 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.
- Tele-Town Hall will also promptly call the relevant customer to inform them of the Traceback request, and that Tele-Town Hall has sent the customer an email requesting specific information related to the investigation.
 - **If the customer does not respond within 24 hours, Tele-Town Hall will suspend the account** – without limiting other actions Tele-Town Hall may take.

¹ See <https://docs.fcc.gov/public/attachments/DA-21-454A1.pdf>.

- Tele-Town Hall 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 Tele-Town Hall's Terms of Service.
- Tele-Town Hall's goal is to comply with all Traceback requests within 24 hours if commercially reasonable, and sooner when practicable.

III. Tele-Town Hall's Know Your Customer ("KYC") Standards

Tele-Town Hall is a voice and text service provider that focuses its operations on the government and non-profit sector of the communications market, with a particular focus on enabling moderated live telephonic town-hall events between elected officials and political candidates and their constituents with enhanced features, such as real-time polling and reporting capabilities. As part of its customer-onboarding process, Tele-Town Hall 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, Tele-Town Hall collects the following customer-identifying information when possible through a STIR/SHAKEN Caller ID Authentication Form:

- Customer organization name,
- Customer email,
- Customer physical address,
- Customer telephone numbers,
- Federal tax ID number (if applicable), and
- Contact person(s) and title.

Once obtaining this information, Tele-Town Hall support and sales staff will attempt to contact all prospective customers during the enrollment process for further vetting or before a customer initiates a Tele-Town Hall event.

IV. Tele-Town Hall's Terms of Use

As part of its customer-onboarding process, all of Tele-Town Hall's customers contractually agree to various terms and conditions, including a commitment to comply with Tele-Town Hall's Terms of Use. Among other things, the Terms of Use provide that:

- Customer accepts full responsibility for and agrees to use Tele-Town Hall® Products and Services in accordance with any and all laws – local, state, and federal – that may be applicable to its use of Tele-Town Hall® Products and Services. Such laws include, but are not limited to, automated call restrictions, privacy laws, and legal calling hours. Customer accepts full responsibility for any violations of laws when using Tele-Town Hall® Products and Services.

- Customer agrees to honor immediately any requests for opt-out or stop further messaging and desist from sending any further message following receipt of any such opt-out or stop request.
- Violation of this Policy may result in termination or suspension of all services provided by Tele-Town Hall® and may also result in civil, criminal or administrative liability or penalties against the client and those assisting the client.

As noted above, Tele-Town Hall's contracts with its customers stipulate that Tele-Town Hall is authorized to suspend and/or terminate all Services in the event of a customer using the Service in violation of these requirements.

V. Telephone Number Authorization and STIR-SHAKEN Capabilities

Tele-Town's service combines various enhanced information services with the outbound calling capabilities provided by underlying carriers. Tele-Town Hall is not subject to STIR/SKAKEN implementation requirements, as it lacks control over the network infrastructure necessary to implement STIR/SKAKEN. That said, Tele-Town's understanding is that its underlying carriers are authenticating Tele-Town Hall's customers' traffic pursuant to STIR/SKAKEN. And as noted above, Tele-Town Hall's end users can only use telephone numbers which they have verified are assigned to them, such that Tele-Town Hall 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

Tele-Town Hall has various monitoring and unlawful traffic 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, Tele-Town Hall by default has its customers scrub their calling lists against a database of wireless telephone numbers. Only if a customer confirms that it has opt-in consent or can lawfully place the calls – for example, when a union or non-profit wishes to conduct a Tele-Town Hall event with its members who have voluntarily released their telephone numbers – can a customer forgo scrubbing their calling lists against the cellphone number database. Tele-Town Hall has also enabled additional features that allow call recipients to place themselves on the calling party's internal DNC list.

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/SKAKEN 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

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

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 calls.” 47 C.F.R. § 64.6305(a)(2).²

Tele-Town Hall notes that, by design, its services are provisioned to significantly curtail end users’ ability to spoof their telephone numbers. Tele-Town Hall’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 Tele-Town Hall’s AUP, Tele-Town Hall’s end users cannot manipulate their caller ID. Thus, by design, Tele-Town Hall’s end users are prevented from using Tele-Town Hall’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, Tele-Town Hall 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, Tele-Town Hall’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.