

Robocall Mitigation Plan

Business Information

Techmode LLC
1091 Centre Rd.
Suite 230
Auburn Hills, MI 48326

Contact Information

Matthew Look
President
248-276-7661
look@techmode.com

Overview

In the Commission's release, *In the Matter of Call Authentication Trust Anchor, Sixth Report and Order and Further Notice of Proposed Rulemaking*, WC Docket No. 17-97 (adopted March 16, 2023) it is stated that all voice service providers ("VSPs") must file robocall mitigation plans ("RMPs") that, among other things, outline "reasonable steps" taken to avoid originating illegal robocalls.

In addition to the "reasonable steps, the FCC requires that a RMP includes:

- "know your customer" procedures;
- a description of any call analytics system used to identify and block illegal traffic; and
- whether a third-party vendor is used and if so, the name of the vendor.

The FCC previously stated that a RMP is sufficient if the detailed practices in the plan can reasonably be expected to significantly reduce the origination of illegal robocalls and the VSP complies with the practices it describes in its filing.

Purpose

Techmode LLC ("Techmode") is a small VSP dedicated to stopping illegal calls from traversing the network and monitoring the calls coming into our network. Techmode has deployed STIR/SHAKEN functions in its network.

Know Your Customer

Techmode employs a robust Know Your Customer (KYC) process to prevent the origination of illegal robocalls and ensure responsible use of our telecommunications services. Our practices include:

1. Customer Identity Verification:

All new clients must submit verifiable business information including:

- Legal business name and physical address
- Tax Identification Number (TIN) or Employer Identification Number (EIN)
- Corporate ownership/management details
- Industry classification and intended use of services

2. Service Use Case Evaluation:
Prospective customers must describe how they intend to use Techmode's services, including their expected call volume, call destinations, and type of content (e.g., customer service, appointment reminders, etc.). High-risk or suspicious use cases are flagged for further review or outright denial.
3. Payment Controls:
We monitor payment patterns and may place restrictions on:
 - The frequency and method of payments (especially for prepaid or high-volume plans)
 - Large or unusual transactions inconsistent with declared business needsThese controls help detect fraud or abuse of service.
4. Ongoing Monitoring and Audit Rights:
Techmode reserves the right to audit client call traffic and service usage. We continuously monitor for patterns indicative of robocalling behavior (e.g., very short-duration calls, sequential number dialing, etc.) and take corrective action when necessary.

Know Your Upstream Providers

In accordance with the Commission's directive in *Advanced Methods to Target and Eliminate Unlawful Robocalls Call Authentication Trust Anchor, Seventh Report and Order In CG Docket 17-59 and WC Docket 17-97, Eighth Further Notice of Proposed Rulemaking In CG Docket 17-59, and Third Notice of Inquiry in CG Docket 17-59* (Rel. May 19, 2023) ¶¶ 49-51, Techmode provides the following information concerning its upstream voice service carrier:

Bandwidth Inc.
2230 Bandmate Way
Raleigh, NC 27607
Isaiah Collins
icollins@bandwidth.com

Techmode has received assurances from its upstream carrier that it has, and will continue to, sign calls transmitted to Techmode and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to Techmode. Techmode and its upstream provider have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Acceptable Use Policy

Acceptable Use Policy ("AUP" or "Policy") describes actions by Users that are prohibited by Techmode, LLC and its affiliates and subsidiaries ("Techmode"). "Users" means any user or Customer of any and all services ("Service" and/or "Services") provided by Techmode pursuant to any applicable customer agreement, including, without limitation, any applicable terms of service, policies and procedures and/or supplements to any applicable agreement(s) (which Users must accept as a condition to receiving any Services from Techmode).

This Acceptable Use Policy is subject to change from time to time with such changes effective upon posting at techmode2.wpengine.com. Techmode encourages Users to review this Policy regularly.

1. Services may be used only for lawful, proper and appropriate purposes.
2. Users must use any Services only in a manner that, in Techmode's sole discretion, is consistent with the purposes of such Services. Users will not engage in any legal or illegal activity that either (i) harms Techmode, the network operated by Techmode, the Services and/or any User, or (ii) interferes with the network operated by Techmode and/or the provision or use of the Services by Techmode or any User.
3. Services may not be used for illegal, improper, and/or inappropriate purposes.
 1. Illegal purposes include but are not limited to:
 - i. using any Service to violate any law, rule, or regulation; or
 - ii. engaging in threatening, abusive, harassing, defamatory, libelous, deceptive or fraudulent behavior.
 2. Improper and/or inappropriate uses include, but are not limited to:
 - posting multiple messages similar in content to Usenet or other newsgroups, listservs, forums, e-mail mailing lists or other similar groups or lists;
 - calling, messaging, storing, posting or transmitting harassing, threatening or abusive materials, e-mail or information;
 - posting or transmitting any information or software that contains a virus worm, cancelbot or other harmful component;
 - without permission from the owner of a system or network, doing any of the following: (a) accessing the system or network, (b) monitoring data or traffic, (c) probing, scanning, and/or testing firewalls, (d) testing the vulnerability of a system or network or (e) breaching the security or authentication routines of a system or network;
 - conducting or forwarding surveys, contests, pyramid schemes, charity requests or chain letters;
 - relaying e-mail in an anonymous fashion or forging any TCP-IP packet header;
 - mailbombing, flooding, overloading, attacking or otherwise interfering with a system or network;
 - sending unsolicited calls, messaging, e-mailings (including, without limitation, commercial advertising and informational announcements) if such unsolicited activities could reasonably be expected to or do in fact provoke complaints;
 - operating a server in connection with the Services in an "open relay" configuration (a configuration whereby a mail server processes email messages where neither the sender nor the recipient is a local user);
 - falsifying User or other identifying information provided to Techmode or to other Users of the Services;
 - use of any Services in violation of any trademark, copyright, or any other intellectual property protection law or provision, or AUP policy of any third party provider;
 - use of any Services for the purposes of engaging in an activity in connection or conjunction with any pornographic and/or adult entertainment industry purpose, regardless of whether such activity is lawfully permitted;
 - auto-dialing or predictive-dialing (sometimes referred to as "robo-dialing");
 - continuous or extensive chat line or conference call participation;
 - use of free conference calling or similar services that Techmode in its sole discretion deems to participate in traffic stimulation practices or schemes that result in excessive charges;
 - use of an open telephone line as a monitoring, intercom or similar service;
 - repetitive and/or continuous messaging or calling to the same destination or number if such

activity could reasonably be expected to or in fact does provoke complaints;

- long duration calls (defined as calls to the same number in excess of four continuous or cumulative hours within a 24 hour period) and/or calls placed to specific numbers / destinations for the purpose of generating charges or fees for or with a third party;
- use of call Services which do not consist of uninterrupted live human voice dialog by and between natural human beings;
- restricting or inhibiting any other User or any other person from using and enjoying the Services and/or the Internet; or
- engaging in any of the foregoing activities by using the services of another provider or third party and channeling such activities through an account provided by Techmode, or otherwise involving the Services or any Techmode account in any way with or without another provider or third party for the purpose of facilitating the foregoing activities.

Remedies:

1. Techmode reserves the right, at its sole discretion, to determine if a Service is being used for any of the foregoing purposes or activities.
2. Violation of this Policy may result in civil or criminal liability, and Techmode in its sole discretion, in addition to any remedy that it may have at law or in equity, may immediately terminate permission for the User to use the Services, or any portion of the Services, and may charge User any applicable rates and cancellation or termination fees. In addition, Techmode may investigate incidents that are contrary to this Policy and provide requested information to third parties who have provided notice to Techmode stating that they have been harmed by a User's failure to abide by this Policy or the policies listed above. Techmode may bring legal action to enjoin violations and/or collect damages caused by any violation of any part of this Policy.
3. Any violations or attempted violations of this Policy by any User (or any third party on behalf of any User) will constitute a violation of this Policy by the User and a material breach of any applicable customer agreement, including, without limitation, any applicable terms of service and/or supplements to any applicable agreement(s).
4. Techmode failure to enforce this policy in every instance in which it might have application does not amount to a waiver of Techmode's rights.
5. IN NO EVENT WILL TECHMODE BE LIABLE TO ANY USER OR THIRD PARTY FOR ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, CONSEQUENTIAL OR OTHER DAMAGES FOR ACTIONS TAKEN OR NOT TAKEN PURSUANT TO THIS POLICY, INCLUDING, WITHOUT LIMITATION, ANY LOST PROFITS, BUSINESS INTERRUPTION, LOSS OF PROGRAMS OR DATA, OR OTHERWISE, EVEN IF TECHMODE WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY IN FAVOR OF TECHMODE IS IN ADDITION TO ANY LIMITATIONS SET FORTH IN ANY WRITTEN AGREEMENT BETWEEN TECHMODE AND ANY APPLICABLE USER AND WILL APPLY WHETHER THE ACTION IN WHICH RECOVERY IS SOUGHT IS BASED IN CONTRACT OR TORT (INCLUDING, WITHOUT LIMITATION, NEGLIGENCE OR STRICT LIABILITY), OR ANY APPLICABLE LAWS.

Telephone Number Analytics

A Telephone Number (“TN”)-based caller identity is the originating phone number included in call signaling used to identify the caller for screening purposes that is uniquely associated with the subscriber. A subscriber is permitted to use a TN as a caller identity if a TN is directly managed by Techmode and/or obtained by Techmode from Techmode’s underlying carrier for use by the subscriber. In most cases, Techmode directly manages the TNs used by its subscribers. Techmode tracks these numbers in its inventory system and monitors the assignment of these numbers. In these cases, TN validation is the inherent result of Techmode’s assignment of the TN to its subscriber.

Analytics for Monitoring Traffic

Techmode uses industry-standard call analytics tools to monitor call traffic patterns in real-time. These tools help us detect abnormal behavior such as high call volumes, short-duration calls, sequential dialing, and high answer-to-seizure ratio (ASR) anomalies—common indicators of illegal robocall activity.

Investigate Suspicious Activity

1. Automated Traffic Monitoring:

Our systems continuously monitor outbound call traffic for patterns commonly associated with illegal robocalls, such as:

- High call volume in short timeframes
- Very short average call durations
- Sequential or random-number dialing
- Low answer-to-seizure ratios (ASR)

2. Traffic Flagging and Alerts:

When suspicious call patterns are detected, automated alerts are triggered and the affected account is flagged for immediate manual review by our compliance team.

3. Manual Investigation:

Our team reviews CDRs (Call Detail Records), call destinations, caller ID usage, and customer history. We may also contact the customer directly to validate call campaigns and request additional documentation or explanations.

4. Temporary Service Restrictions:

If warranted, we may temporarily block outbound calling or restrict traffic on specific numbers or trunks until the issue is resolved.

5. Traceback Cooperation:

We fully cooperate with traceback requests from the Industry Traceback Group (ITG) and law enforcement. When a traceback request is received, we prioritize the investigation and provide all relevant information promptly. Techmode will respond to traceback requests within 24 hours of receiving same.

6. Corrective Action and Enforcement:

If we confirm that a customer is generating illegal robocalls, we take immediate enforcement action, which may include service suspension, termination, and/or notification to upstream carriers and regulators.

No third-party vendors are involved in deploying Techmode's analytics.

Blocking

We implement automatic rate limiting and can block outbound traffic that meets the criteria for suspicious robocalling. We also participate in traceback efforts when flagged by industry or government bodies.

Plan Updates

This plan and industry best practices must evolve to response to the dynamic nature of mitigating illegal robocalling. Techmode will monitor industry best practices and continuously improve our internal processes to ensure this plan, and our system adapt to this ever-changing issue.

In the event of any material change to this plan, Techmode will republish it to employees, consultants and contractors and file such an update to the FCC Robocall Mitigation Database within ten (10) days of such update.

Certification of Matthew Look

I, Matthew Look, President of Techmode LLC ("Techmode"), do hereby certify, under penalty of perjury, the following:

- (1) Techmode has fully implemented STIR/SHAKEN in the IP portions of its network.
- (2) Techmode's business name and primary address are as follows:
Techmode LLC
1091 Centre Rd.
Suite 230
Auburn Hills, MI 48326
- (3) Techmode's d/b/a is TechmodeGo.
- (4) Techmode has not previously used any other d/b/a names.
- (5) Techmode has not been subject to an FCC enforcement proceeding or have been forbidden to file in the Robocall Mitigation Database.
- (6) The name, title, department, business address, telephone number, and email address of the individual responsible for addressing robocall-related issues are listed in the above robocall mitigation plan.
- (7) Techmode's role in the call chain is that of a voice service provider with a STIR/SHAKEN obligation.
- (8) Techmode's operator company number is 442L.

/s/Matthew Look