

Robocall Mitigation Plan

Municorn Limited

Effective date: March 24, 2025

1. Overview

Municorn Limited ("Municorn" or "We") provides users with a service phone number for personal and professional use, all with no need for an additional SIM card. Our app enables users to select a second phone number and make calls. Municorn delivers voice, messaging, and related services via its own mobile applications.

Municorn has closely followed the FCC's implementation of the Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act. Such implementation includes the required employment of STIR/SHAKEN caller ID authentication technology in the Internet Protocol (IP) portions of the networks.

Municorn has certified its compliance in the Robocall Mitigation Database and has instituted a Robocall Mitigation program to ensure that Municorn is not originating illegal robocalls.

The following policies apply to all users of Municorn and comprise our Robocall Mitigation Plan to avoid originating illegal robocall traffic from our network.

2. STIR/SHAKEN Compliance

Pursuant to 47 CFR 64.6305(d)(2)(i), Municorn qualifies for an exemption from STIR/SHAKEN implementation due to a lack of control over the network infrastructure necessary to implement the technology.

Municorn does not directly implement STIR/SHAKEN but ensures compliance through Telnyx, our primary VoIP provider, which has fully implemented STIR/SHAKEN and certified its compliance with the FCC Robocall Mitigation Database.

3. Contract Requirement (Messaging and Calling Policy)

All new users are contractually obligated to abide by our Messaging and Calling Policy and Terms of Use prior to accessing and using our mobile applications. Municorn's Messaging and Calling Policy clearly stipulates that our services cannot be used for illegal, improper, and/or inappropriate purposes. Illegal purposes include but are not limited to using our service in connection with violations of any laws, or engaging in threatening, abusive, harassing, defamatory, libelous, malicious, deceptive, or fraudulent behaviour.

Among other improper and/or inappropriate uses, Municorn's Messaging and Calling Policy prohibits sending unsolicited calls and messages (including, without limitation, commercial advertising and informational announcements) if such unsolicited activities could reasonably be expected to or do, in fact, provoke complaints.

Municorn's Messaging and Calling Policy states that if Municorn receives a request from a traceback administrator or a VoIP provider for information about suspicious robocalls that have been sent through our mobile applications, Municorn will investigate it and promptly respond within 24 hours to the

request in good faith. Also, Municorn may terminate a user's agreement, any service, or both immediately if the user fails to comply with our policy.

4. Call Blocking

If our users send illegal robocall traffic Municorn may use its VoIP provider's call blocking solutions, which include:

- Inbound Call Screening with SHAKEN/STIR validation.
- Spam Call Detection to prevent fraudulent call origination.

5. Users Monitoring & Fraud Prevention

If fraudulent activity is detected, Municorn may:

- Warn the customer and require additional verification.
- Suspend or terminate services for severe or repeated violations.
- Report violations to relevant authorities.

6. Investigation of Suspicious Activity & Traceback

Municorn diligently monitors its system and will investigate any suspicious traffic to ensure compliance with robocall mitigation technologies and minimizing fraud origination. We act promptly upon detecting traffic that appears to be robocall activity to determine whether it has been preauthorized as legitimate (i.e. authorized political, non-profit, reverse 911 or fully-opted-in traffic).

Any alert sent to Municorn through internal monitoring, tracebacks, and vendor alerts (from our VoIP provider) is properly reviewed by our fraud team. We request a specific and detailed explanation from the user and insist on immediate corrective action. If corrective action is not taken in a timely manner, Municorn will take necessary action to prevent further occurrences, including removing the user from our mobile applications.

7. Law Enforcement cooperation

Municorn cooperates fully with investigative authorities, industry traceback groups, the FCC, and the official consortium designated to lead private traceback efforts.

8. Robocall Mitigation Plan Updates

Municorn will periodically update this Robocall Mitigation Plan to ensure compliance with evolving FCC regulations and industry standards. If any changes occur, this plan will be updated accordingly.

9. How to Contact Us

If you have any questions or concerns about this Robocall Mitigation Plan, please contact us:

legal@municorn.com