

Ringover Inc Robocall Mitigation Plan

Submitted December 2024

Ringover Inc - FCC Registration Number: 0031063183

1. Summary.....	3
2. Robocall Mitigation Practices.....	3
2.1. Ringover Tools for Outbound Calling.....	3
2.2. Usage limits.....	3
2.3. Pattern identification for suspected fraud.....	3
2.4. Content analysis of telephone conversations.....	4
3. Call Authentication.....	4
4. Identity, Address and VPN Verification.....	5
5. Payment fraud.....	5
6. “Know Your Upstream Provider”	5
7. Complaint Management and Coordination with Regulators.....	5
Point of Contact for Robocall Mitigation.....	5

1. Summary

Ringover Inc is a voice service provider revolving around the use of Ringover, a software-based communication platform that enables customers to make and receive calls.

Ringover operates within a controlled environment, where users' calling activities must be conducted within the Ringover ecosystem under its predefined rules and legal limitations, which enables enforcement of the fraud prevention practices detailed in this document, including robocall mitigation.

2. Robocall Mitigation Practices

Ringover Inc is committed to ensuring its network is not used to transmit illegal robocalls or any kind of fraudulent call. We have developed effective analysis and monitoring tools to identify and block calling patterns, outlined below.

2.1. Limiting Outgoing Calls with Ringover

Two limitations on call origination constitute the first line of defence against illegal robocalls, or any kind of large-scale outbound calling:

- Ringover does not provide tools facilitating robocalls; users have to perform manual actions to make calls, and there is a default limit of 2 concurrent outbound channels per user;
- Similarly, Ringover does not provide tools allowing automated systems to emit calls and broadcast pre-recorded messages.

2.2. Monitoring Customer's Usage of Outbound Calling

Ringover Inc applies strict limits to how our customers can utilize our platform, and monitors the usage of all our customers. Tools have been put in place to automatically suspend offending accounts. Our teams are also able to investigate and block accounts manually when suspicious behaviour occurs. These measures have proven effective in the past and have led to the termination of several accounts.

- **Daily usage limit:** there is a default daily limit in the number of calls a user can emit before being automatically blocked for the next 24 hours.
- **Detection of a high rate of short calls:** this is a typical pattern of unsolicited prospecting, leading to automatic blocking of users.
- **Analysis of outbound destinations:** high-risk destinations are identified and may lead to blocking if the thresholds set are exceeded.

- **Hacking detection:** access to user accounts via unusual or suspicious IP addresses is flagged as being susceptible to hacking. Our teams review these alerts so that they can take action in collaboration with the affected users.
- **Content analysis of telephone conversations:** Ringover Inc has developed an internal system of automated analysis of telephone conversations, designed to detect fraudulent use. Our system automatically transcribes conversations, then a language processing algorithm automatically determines the business activity corresponding to the telephone conversation. If a risky activity is detected (e.g. banking/finance), our teams are notified immediately and carry out an in-depth investigation of the account concerned, checking in particular the consistency between the business activity detected by our artificial intelligence and the activity indicated in the trade and companies register. In the event of inconsistency, the account is immediately suspended. This system has proved extremely effective, as the fraudulent user is automatically detected by the very fact that he is carrying out his fraudulent activity by telephone.

All the measures detailed above help protect our network by detecting and blocking unwanted traffic and usage.

3. Call Authentication

Ringover Inc has implemented the STIR/Shaken framework across all IP-based portions of its network. All outgoing calls are authenticated with STIR/SHAKEN protocols, ensuring their legitimacy.

Moreover, customers cannot use arbitrary phone numbers. Customers can only originate calls using numbers clearly associated with their Ringover account. Combined with the implementation of STIR/Shaken, the attestation levels of calls signed by Ringover Inc can be fully trusted on the telephone network.

4. Identity, Address and VPN Verification

Ringover requires all new customers to undergo an ID check before they can benefit from its services, to ensure they do not pose a risk of originating calls that do not comply with our terms of service.

This check is carried out via Veriff, a third-party solution which combines artificial intelligence with manual checks. The platform asks the user to take a photo of their ID, checking that it is an original and not a copy (in which case authentication is refused), and then a video of their face, in order to verify biometric consistency between the person holding the ID and the person presenting it. Several financial institutions such as Wise and Visa rely on the same solution for their platforms.

In addition, our teams manually check the addresses given by the customers against the proof of address provided at the time of subscription. Any discrepancy between the two will result in an immediate refusal to use the service.

Our teams also report VPN or proxy use on our customer account management tool.

5.Payment Fraud

Ringover Inc processes payments via Stripe's "Radar for Fraud", a tool designed to detect and prevent fraudulent transactions in real-time. Proactively blocking potentially fraudulent transactions strengthens our other fraud prevention measures by denying access to customers with malicious intent.

6.“Know Your Upstream Provider”

Ringover INC interconnects with the providers listed below, all of which are registered on the Robocall Mitigation Database and take part in the ongoing efforts to prevent illegal or fraudulent use.

- Bandwidth Inc (FRN 0015443773)
- Belgacom International Carrier Services SA (FRN 0024904963)
- DIDWW Ireland Limited (FRN 0031090475)
- Sinch America, Inc. (FRN 0031078843)
- Orange S.A. (FRN 0031077514)
- Voxbone SA (FRN 0031092331)

7.Complaint Management and Coordination with Regulators

Ringover cooperates with the authorities when a requisition is requested against one of our customers. Ringover is able to process such requests quickly, suspending all activity on the accounts concerned.

Ringover Inc intends to fully cooperate with the FCC and other industry organizations on their robocall mitigation efforts, and commits to responding to any traceback request within 24 hours. These requests can be submitted via noc@ringover.com.