

# Robocall Mitigation Policy

## 1. Purpose

The purpose of this Robocall Mitigation Policy is to outline the measures and procedures our organisation will implement to detect, prevent, and mitigate illegal and unwanted robocalls. This policy ensures compliance with relevant regulations, protects our Customers from fraud and nuisance, and maintains the integrity of our communication services.

Pursuant to the provisions of 47 C.F.R. § 64.6305, adopted by the Federal Communications Commission (FCC) which require all “voice service providers” to establish a “robocall mitigation plan”, this document sets forth Xoom Ltd’s current policies and procedures designed to reduce or eliminate outbound illegal robocalls originating on its Network. These policies and procedures as constituting “reasonable steps” to avoid the origination of illegal robocalls on our Network. In addition to following steps, we commit to responding to all traceback requests from the FCC via our upstream carriers, law enforcement, and the Industry Traceback Group (ITG), and to cooperate with such entities in investigating and stopping any illegal robocallers that may use its service to originate calls.

## 2. Scope

This policy applies to all employees, Customers, Wholesale Partners, Referral Partners and third-party service providers involved in the transmission of Voice Calls through our telecommunications network.

## 3. Definitions

- **Robocall:** An automated telephone call that delivers a recorded message.
- **Illegal Robocall:** Any robocall that is made in violation of applicable laws and regulations, including those that involve fraudulent schemes or fail to obtain necessary consent from the called party.
- **Unwanted Robocall:** Any robocall that the recipient did not consent to receive, including telemarketing calls to numbers on the National Do Not Call Registry.

## 4. Regulatory Compliance

Our organisation commits to complying with all relevant laws and regulations regarding robocalls, including but not limited to:

- Ofcom and other industry codes of conduct which can be found at <https://comms council.uk/>
- Federal Communications Commission (FCC) regulations

As a UK business we are not part of the STIR/SHAKEN initiative and therefore the carrier will attest only that they know where they have received the call from (Gateway Attestation C).

We have not implemented the STIR/SHAKEN authentication framework on any portion of our Network however all calls originating on our Network are subject to the procedures set forth in this Robocall Mitigation Policy which are intended to prevent any Customer from using our service to originate illegal robocalls.

## **5. Mitigation Measures**

### **5.1 Call Authentication**

Authentication to verify the caller ID information on calls originating from our Network and ensure the accuracy of the caller ID for calls terminating on our Network.

### **5.2 Traffic Monitoring and Analysis**

Regularly monitor and analyse call traffic patterns to detect unusual or suspicious activity that may indicate robocall campaigns. This includes:

- High call volume patterns
- Repeated short-duration calls
- Unusual calling patterns to specific geographic locations

We monitor the usage of our Network and examine call detail records (CDRs) on a recurring basis for the purpose of detecting suspicious call activity and/or calling patterns. When Network usage patterns consistent with illegal robocalls are detected or we otherwise suspect illegal robocalling or spoofing is taking place on our network, we immediately seek to identify the party that is originating, terminating, or routing these calls so that it may take appropriate action. The actions taken may include, but are not limited to: initiating a traceback investigation; verifying that the originating customer owns or is authorised to use the Caller ID number; determining whether the Caller ID name sent to a receiving party matches the customer's corporate name, trademark, or d/b/a name; terminating the party's ability to originate, terminate, or route calls on our network; and providing notice to relevant authorities and upstream providers. As part of this Policy to mitigate and prevent any originating robocalls we are committed to early identification and investigation of possible robocalling situations. In monitoring usage of our Network, particular attention is given to:

- (1) higher than normal subscriber traffic volume including large bursts of traffic in small timeframes or inconsistent volumes of traffic (spikes in usage);
- (2) originating calls of short duration and low call completion percentages;
- (3) originating calls with sequential called to number dialling patterns; and
- (4) repeated calls made to do-not-call registry or invalid numbers.

### **5.3 Blacklisting**

Maintain and update a blacklist of known robocallers and sources of illegal robocalls or any malicious IP addresses. Automatically block calls from these sources.

### **5.4 Whitelisting**

Maintain and update a whitelist of legitimate callers, such as emergency services and trusted businesses, to ensure their calls are not mistakenly blocked.

### **5.6 Reporting and Escalation**

We will cooperate with the FCC, law enforcement and the (ITG) on all traceback requests and investigations. To allow for timely and comprehensive law enforcement response efforts against illegal robocallers, we will dedicate sufficient resources to promptly complete and provide responses to all traceback requests received from our upstream carriers, the FCC, law enforcement and/or the ITG, and commits to fully responding to any traceback 2 request received within 24 hours after receiving the same.

In addition to this we have a clear process for reporting suspected illegal robocalls to relevant authorities, including the FCC. This process includes:

- Documentation of the suspected robocall activity
- Immediate notification to regulatory authorities as required
- Immediate disconnection of suspected services/Customers
- Cooperation with investigations

### **5.7 Customer Vetting Practices**

As a means of preventing or minimising the origination of illegal robocalls through our voice services, we use best practices in vetting the identity of all of our voice service subscribers, (including any entities that are purchasing our services for resale). The subscriber vetting process is intended to help determine the legitimacy of a Customer for the purpose of establishing a service relationship. Generally, Xoom looks to confirm the identity of Customers using its voice services through collecting information such as registered company information, physical customer location, contact person(s), country of incorporation, and the nature of the Customer's business. Our efforts to vet Customers occurs during the process of provisioning Customer requested Services (for example in appropriately sizing the facilities to their claimed intended use), executing the required Service Agreements, and granting the Customer the right to use telephone number resources. End users, comprising larger businesses with more complex service configurations, are generally recognized as presenting a higher risk of perpetrating illegal robocalls and thus those Customers, at Xoom Ltds discretion, may be subject to an additional review, including a more stringent background check and possibly a site visit. To take affirmative, effective measures to prevent new and renewing Customers from originating illegal calls, we use Service Agreements and Acceptable Use Policies as a means of preventing new and existing subscribers from using voice and connectivity services in ways that would be in violation of regulations or laws, or to engage in deceptive

or fraudulent activity. These documents governing use of our provided services include terms indicating specifically to all Customers that their services should not be used for the purpose of making illegal robocalls, and that Xoom reserves authority within its Service Agreements to suspend or terminate a subscriber's voice service for violating applicable service-related terms. We have established a routine process for monitoring the usage and quality of our network facilities and conduct recurring and timely reviews of our call detail records (CDRs) to facilitate early identification of unusual or suspicious calling activity or patterns that may indicate use of our network for originating illegal robocalls. In those instances where we identify activity or a pattern consistent with illegal robocalls the Customer will be contacted within twenty-four hours for further investigation and possible action.

## **5.8 Telephone Number Validation Practices**

Telephone Number Validation refers to the confirmation of the Customer or end-user right to use a telephone number in connection with their subscribed voice service(s). In accord with industry best practices, we have procedures in place to confirm the calling customer's right to use a telephone number. Specifically, a subscriber of the services is permitted to use a telephone number as their caller identity if a number is directly managed by Xoom and/or obtained by Xoom via an underlying partner.

## **5.8 International Call Originators**

Xoom Ltd is not currently an international voice services provider. If at any time we do sell our services to customers which are international call originators using North American Numbering Plan resources, we will familiarise ourselves with and develop best practices for vetting such customers and performing telephone number validation on all international originated calls.

## **5.9 Know your upstream provider procedures**

The number of upstream providers used by Xoom Ltd to receive and deliver originated voice calls for termination are limited. We have long standing relationships with these upstream providers and maintain our awareness of the nature of their businesses and the legitimacy of their call transmission services. In the interest of providing the highest quality services to our voice service customers, we are committed to taking those steps necessary to ensure that any upstream providers are equally committed to monitoring their networks and preventing their use for the transmission of illegal robocalls. This includes the use of robocall prevention language in any contracts we may directly have with any upstream provider entities.

## **6. Enforcement**

Any employee, Customer employees, Wholesale Partner, Referral partner found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment or Service Agreements. Third-party service providers found to be in violation may be subject to contract termination and legal action.

## **7. Review and Update**

This policy will be reviewed and updated annually or as required by changes in relevant laws and regulations. Any updates to the policy will be communicated to all employees, Wholesale Partner, Referral partner and third-party service providers, as required.

## **8. Contact Information**

For questions or concerns regarding this policy, please contact us:

Telephone: 0333 110 3000

Email: [hello@xoomtalk.com](mailto:hello@xoomtalk.com)

Post: Xoomtalk, PLatf9rm Hove Town Hall, Church Road, Hove, BN3 2AF

Web: [www.xoomtalk.com](http://www.xoomtalk.com)

---

By implementing and adhering to this Robocall Mitigation Policy, Xoom Ltd aims to protect our Customers, maintain the integrity of our telecommunications network, and comply with regulatory requirements regarding robocalls.