

Robocall Mitigation Plan

Business Information

Exridge Pte Ltd
31 Rochester Drive, # 24-00
Singapore 138637

Contact Information

Kerry Weir
Founder/CEO
646.461.4696
Kerry.weir@exridge.com

Overview

The FCC requires that all small voice service providers ("VSPs") certify in the Robocall Mitigation Database that they have implemented a Robocall Mitigation Plan ("RMP") to ensure that they are not originating illegal robocalls.

The FCC requires that VSPs develop a RMP that:

- details the reasonable steps taken to avoid originating illegal robocalls;
- demonstrates a commitment to respond to traceback requests to cooperate with investigators and stopping illegal robocalls; and
- is filed in the Robocall Mitigation Database.

The FCC states 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

Exridge Pte Ltd ("Exridge") is dedicated to stopping illegal calls from originating in our network and monitoring the calls coming into our network. This document delineates Exridge's RMP.

Know Your Customer ("KYC")

The accurate identification of a subscriber in the STIR/SHAKEN ecosystem is tied to a telephone number-based caller identity associated that subscriber. A subscriber is an entity that has a business relationship with Exridge in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

Exridge has two types of clients, and different KYC programs for each category.

1) Clients that we manage and develop services for, who sell to end users. We have a written sales agreement with these subscribers which requires them to provide their Corporation Number ("CN"). We can use the CN to obtain additional information, such as physical business location, contact person(s) and other pertinent material.

b) Direct End Users. We ask for their mobile number at sign up and send an SMS passcode to this number so they can complete registration. In this manner their numbers are verified. When we

provide virtual numbers, we have a KYC module within the app where users upload a copy of their passport and a utility bill.

Acceptable Use Policy ("AUP")

Exridge provides the following language in its customer service contracts:

The Customer must comply with Schedule 2 (Acceptable Use Policy), and must ensure that all persons using the Hosted Services with the authority of the Customer or by means of an administrator Account comply with Schedule 2 (Acceptable Use Policy).

Schedule 2 (Acceptable Use Policy)

Customers are prohibited from transmitting on or through any of Exridge's services, any material that is, in Exridge's sole discretion, unlawful, threatening, abusive, libelous, or encourages conduct that would constitute a criminal offence, give rise to civil liability, or otherwise violate any local, national or international law, statute or regulation. Exridge services may only be used for lawful purposes.

Customers must provide information to their end users about safeguarding their account passwords to prevent unauthorized access to their account. Exridge will cooperate fully with investigations of violations of systems or network security at other sites, including cooperating with law enforcement authorities in the investigation of suspected criminal violations.

Exridge reserves the right to check the security of a Customer's equipment or devices used to connect to its network if it reasonably believes that equipment on the customer's network may be at risk from external attack (hacking) or if they believe that its terms and conditions of use are not being followed.

Telephone Number Authorization

A Telephone Number ("TN")-based caller identity is the originating phone number included in call signaling used to identify an outbound 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 Exridge and/or obtained by Exridge from one of Exridge's underlying carriers for use by the subscriber. In most cases, Exridge directly manages the TNs used by its subscribers. Exridge tracks these numbers in its inventory system and monitors the assignment of these numbers. In these cases, TN validation is the inherent result of Exridge's assignment of the TN to its subscriber.

If a subscriber wishes to use a TN as a caller identity and that TN is not directly managed by Exridge, then TN validation is necessary. If a subscriber's end-user can provide a valid letter of authorization that they are the authorized user of such TNs, Exridge will attest calls originated with these TNs.

When originating a call, Exridge checks the calling party number against Exridge's inventory and will not attest the call unless the calling party number is a TN that has been properly validated.

Monitoring

Exridge has a monitoring and reporting system in place to analyze high-volume voice traffic to identify and monitor patterns consistent with robocalls. Our server-based monitoring system alerts

us to calling patterns with unusual spikes, traffic patterns, or attempted use of non-validated ANIs to detect patterns consistent with illegal robocalls.

If Exridge detects a calling pattern consistent with illegal robocalls, we will identify the party that is using our network to originate those calls and will take appropriate action. Taking appropriate action may include, but is not limited to, initiating a traceback investigation, verifying that the originating subscriber owns or is authorized to use the Caller ID number, and suspending or terminating the party's ability to originate calls on our network.

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, our risk prevention team is alerted which follows the defined procedures on investigating such subscribers.

The procedures established include but are not limited to:

- checking recent and past call detail records and benchmark against expected trends;
- checking recent and past account activity and purchases;
- investigating if any system issue generates the strange behavior;
- verifying that the call originating path is valid; and
- contacting the subscriber to understand his or her particular use case and validate that the activity belongs to that subscriber.

Exridge follows Industry Traceback Group ("ITG")-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, Exridge will devote sufficient resources to provide prompt and complete resources to traceback requests.

Blocking

Exridge will implement Do Not Originate requests it receives from the ITG. Exridge has mechanisms to automatically block suspicious calls using internal analytics. If Exridge's monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, Exridge will take appropriate action which may include suspending or terminating the subscriber's use of Exridge's network. Exridge will cooperate with Investigative Bodies (provide a single point of contact to address traceback requests from law enforcement (including the state attorney general's office), to the FCC, and/or the ITG; as well as documenting requests & actions taken in response thereto.

Plan Updates

This plan and industry best practices must evolve to response to the dynamic nature of mitigating illegal robocalling. Exridge 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, Exridge 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.