

Robocall Mitigation Plan

T&I Net Communication Co.,Ltd.(" T&I Net") is a contact center provider, T&I Net dedicated to stopping illegal calls from originating in our network and monitoring the calls coming into our network. T&I Net with traceback requests received directly from carriers, industry associations, and law enforcement.

1. Check our customers

The accurate identification of a user in the STIR/SHAKEN ecosystem is tied to a telephone number-based caller identity associated with that user. A user is a company that has a business relationship with T&I Net in which we transmit, originate, and/or terminate calls based on behalf of the user.

1.1. New user

All new users go through identity verification protocols which are a mixture of algorithmic check and manual verify. T&I Net ensures the new user has company entity and subsequent background verifications are carried out using legal and compliance team to ascertain a reasonable legitimacy of the business. Information collected as part of these checks, includes but is not limited to: company name, business license, contact name, contact phone number, contact ID card, email address, website, nature of business, brand name and trademark.

2. Acceptable Use Policy

T&I Net maintains an Acceptable Use Policy ("AUP") that user must sign up to, before being permitted to use T&I Net's service. Among other things, this AUP prohibits:

- providing altered, deceptive, or false information about the identity of the sender or the origin of a message or phone call;
- violating any applicable local, state, or country law;
- violating applicable industry accepted guidelines;
- using T&I Net's service to engage in or in connection with fraudulent activities.

T&I Net's contractual terms with users specify that T&I Net may take action up to suspension or termination of service for violation of the AUP.

3. Telephone Number Authorization

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 user. A user is permitted to use a TN as a caller identity if a TN is obtained by T&I Net from one of T&I Net's underlying carriers for use by the user. T&I Net manage the assignment of these numbers and monitor these numbers in its inventory system. In these cases, TN validation is the inherent result of T&I Net's assignment of the TN to its user.

If a user wishes to use a TN as a caller identity and that TN is not directly managed by T&I Net, T&I Net will block the call. When originating a call, T&I Net checks the calling party number against T&I Net's inventory and will not make the call unless the calling party number is a TN that

has been properly validated.

4. Monitor Traffic with Analytics

T&I Net has thresholds and subsequent alerting mechanisms in place for possible fraud detection based on the following parameters:

- daily duration minutes comparison for sudden spike
- total count of daily calls
- daily call average answer rate

Account Managers are alerted based on a risk breach based on the above parameters.

In addition to the above, T&I Net is in the process of implementing Dynamic Traffic Analysis which will identify behaviors which indicate illegal call activity.

Examples of calling patterns monitored:

- large volumes of short duration and incomplete calls;
- multiple overlapping calls on the same account is a risk of not having a single user using the service;
- velocity on initiate calls (synchrony intervals, quick dialing calls);
- recent volumes (last 60 min) vs weekly trends;
- number of unique destination numbers in a time frame;
- number of unique source numbers in a time frame;
- anomalies in call duration distribution (most calls having similar duration are not representative for business service usage).

The implemented detection rules will also be reviewed and updated from time to time in order to increase the effectiveness of the monitoring system.

5. 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 user.

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 IP address activity;
- investigating if any system issue generates the strange behavior;
- verifying that the call originating path is valid;
- contacting the user to understand his particular use case and validate that the activity belongs to that user.

T&I Net follows best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, T&I Net will devote sufficient resources to provide prompt and complete resources to traceback requests.

T&I Net will investigate suspicious activity found by its monitoring systems or reported to T&I Net by users or third parties. The investigation could potentially result in opening a traceback request or with T&I Net contacting a user to correct improper use of the platform, or, if the user does not respond or comply, to block their use of the platform.

For all new and renegotiated T&I Net contracts governing the transport of voice calls, T&I Net will use best efforts to contractually require T&I Net's user to cooperate in traceback investigations by

identifying the upstream provider from which the suspected illegal robocall entered our network.

6. Plan Updates

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