

Creative World Prime Robocall Mitigation Plan Purpose

Creative World Prime (“CWP”) is dedicated to stopping illegal calls from originating in our network and monitoring the calls coming into our network consistent with Federal Communications Commission (“FCC”) regulations.

CWP has implemented the STIR/SHAKEN call authentication protocol in the IP portions of its network. STIR/SHAKEN does not, however, cover the TDM portions of CWP’S network. Therefore, CWP has also adopted the policies and procedures set forth in this document to comply with the FCC’s anti-robocalling regulations. This document defines CWP’S Robocall Mitigation plan.

“Know Your Customer” (“KYC”)

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

CWP’S KYC program requires a signed contract with our subscriber. Prior to signing a contract, CWP confirms a subscriber’s identity by vetting a subscriber directly or by using a third-party vetting service. The vetting process includes collecting information such as:

- physical business location,
- contact person(s),
- state or country of incorporation,
- federal tax ID,
- nature of the customer’s business.

Telephone Number Authorization

For the purposes of this plan, a Telephone Number (TN)-based caller identity is defined as the originating phone number included in call signaling used to identify the caller for call screening purposes that is uniquely associated with a subscriber. A TN used for caller identity may or may not be associated with the subscriber’s account with the responsible party.

A subscriber is permitted to use a TN as a caller identity if a TN is directly managed by CWP and/or obtained by CWP from one of CWP’S underlying carriers for use by the subscriber. In most cases, CWP directly manages TNs used by its subscribers. CWP tracks these numbers in its inventory system and monitors the assignment of these numbers. In these cases, TN validation is the inherent result of CWP’S assignment of the TN to its subscriber.

When originating a call, CWP checks the calling party number (also called the ANI) against CWP'S inventory and will not attest the call unless the calling party number is a TN that has been properly validated.

Monitoring

CWP has monitoring and reporting systems in place to analyze high-volume voice network traffic to identify and monitor patterns consistent with Robocalls. Our monitoring systems alert on calling patterns with unusual spikes, traffic patterns, or attempted use of non-validated ANIs to detect patterns consistent with illegal Robocalls and attempts at illegal call spoofing.

If CWP detects a pattern consistent with illegal Robocalls, or we have reason to suspect illegal Robocalling or spoofing is taking place over our network, we will seek to identify the party that is using our network to originate, route, or terminate these calls and take appropriate action.

Taking appropriate action may include, but is not limited to, initiating a traceback investigation, verifying that the originating commercial customer owns or is authorized to use the Caller ID number, and suspending or terminating the party's ability to originate, route, or terminate calls on our network.

Investigation of Suspicious Activity and Traceback

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

CWP will investigate suspicious activity found by its monitoring systems or reported to CWP by consumers or third parties. The investigation could potentially result in opening a traceback request or with CWP contacting a subscriber to correct improper use of the platform, or, if the subscriber or subscriber's EndUser does not respond or comply, to block their use of the platform.

For all new and renegotiated CWP contracts governing the transport of voice calls, CWP intends to contractually require CWP'S subscribers to cooperate with in traceback investigations by identifying the upstream provider from which the suspected illegal Robocall entered our network.

Blocking

When it is administratively feasible, CWP will implement Do Not Originate ("DNO") requests it receives from the ITG.

If CWP'S monitoring systems identify suspected Robocalling patterns that are confirmed with further investigation, CWP will take appropriate action which may include suspending or terminating the subscriber's or End-User's use of CWP'S network.

Plan Updates

This plan and industry best practices must evolve to respond to the dynamic nature of mitigating illegal Robocalling. CWP will monitor industry best practices and continuously improve our internal processes to ensure this plan and our systems adapt to this ever-changing issue.