

SKYWIRE ROBOCALL MITIGATION PLAN

Below is the Robocall Mitigation Plan (the “Plan”) for Xchange Telecom LLC d/b/a Skywire Networks (“Skywire”) that applies to all calls that originate or terminate on Skywire’s network. This Plan will be submitted to the FCC’s Robocall Mitigation Database and will be adapted to adjust to the latest laws, regulations, and industry best practices. Skywire will update this Plan within ten (10) business days following the date of any changes to the Plan.

STIR/SHAKEN Implementation Status

Skywire is a voice service provider with a STIR/SHAKEN implementation obligation serving end-users.¹ As of February 22, 2024, Skywire has completed implementation of the STIR/SHAKEN authentication framework on the IP portions of its network. For the TDM portions of Skywire’s network that are not capable of STIR/SHAKEN implementation because they cannot initiate, maintain, carry, process, and terminate SIP calls, Skywire relies on the continuing extension provided under Section 64.6304(d) of the FCC’s rules.²

As work to develop a non-IP caller identification authentication solution has been underway, Skywire independently has developed a protocol to:

- Identify on-net, non-IP (TDM) customers and set an attestation appropriately identifying the caller as a known caller.
- Identify off-net, non-IP customers received via intermediate provider and set attestation appropriately identifying caller as a known caller via an intermediary.
- Identify non-IP customers’ calls from either of the above, that did not originate from the customer (*i.e.*, a forwarded call) and set attestation appropriately identifying the caller as an unknown caller.

Terms of Use/Acceptable Use Policies

Skywire’s terms of service for voice offerings prohibits use of the service for unlawful purposes, permits Skywire to monitor use of the service for compliance, and allows for termination of the service at Skywire’s discretion.³ The terms allow Skywire to monitor customer usage to determine whether abnormal, unreasonable, or impermissible use is occurring based upon use of the service as evaluated in comparison to other similarly situated customers. Under the terms, Skywire maintains the right (in its sole discretion) to require customers to terminate their service plans in the event of use of the service, any feature and/or any device in a way that is inconsistent with the normal use of the service. In the event that a customer does not immediately conform its use to acceptable levels, Skywire retains the right to immediately suspend the infringing customer’s account and service and also retains the right to remove or block communications upon suspicion of a violation of the terms. Finally, Skywire retains the right to forward the relevant communication (including the customer’s identity) to the appropriate authorities for investigation and prosecution in the event that Skywire believes that a customer’s use is for an unlawful purpose.

New and Renewing Customer Vetting Process

Before commencing services for new customers, or renewing service contracts for existing customers, Skywire obtains the following information regarding our customers:

- Customer identity
- Contact information

¹ Skywire does not act as a Gateway Provider or Non-Gateway Intermediate Provider as defined by the Commission’s rules. *See* 47 C.F.R. §§ 64.6300(d), (i).

² *See* 47 C.F.R. § 64.6304(d) (continuing extension of the implementation deadline for non-IP networks).

³ *See* <https://skywirednetworks.com/termservice/central-office/>.

- Service address
- Billing address
- Credit history

For business customers, Skywire also confirms that the business has a record of conducting legitimate business activity (including use of a legitimate business name) before we will commence services. In addition to confirming the identity of the business customer, Skywire's team will conduct research using publicly available sources (including the customer's website and other internet-based resources).

Upstream Provider Vetting Process

All calls accepted by Skywire from other carriers are delivered by Tier 1 service providers or carriers terminating to Skywire's conference or IVR services. Skywire only accepts traffic from upstream providers who have been vetted and are known carriers. Among other information obtained from upstream carriers, Skywire obtains the provider's identity and address(es). All calls received from other carriers also are queried through the Bulk Solutions Robocall Mitigation Solution described below.

Monitoring Customer Usage

Skywire 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 provide alerts on calling patterns with unusual spikes, traffic patterns, or attempted use of non-validated Telephone Number ("TN") to detect patterns consistent with illegal robocalls.

If Skywire detects a pattern consistent with illegal robocalls, or if 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, which may include validating that the originating party is authorized to use the TN and/or suspending calling party's ability to originate, route, or terminate calls on Skywire network.

Traceback Cooperation

Skywire commits to responding fully and within 24 hours to all traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG). Skywire also commits to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

Bulk Solutions Robocall Mitigation Solution Overview

In addition to its usage monitoring efforts undertaken in-house, Skywire uses a robocall mitigation process provided by third-party vendor Bulk Solutions (the "Bulk Solutions Process"). The Bulk Solutions Process "combines behavioral analytics, caller authentication and verification to help accurately identify robocalls, mitigate fraudulent robocalls, caller ID spoofers and call scammers."⁴

The Bulk Solution Process provides robocall scoring based on the annual +100B carrier calls that Bulk Solutions processes as part of the Caller Name service. STIR/SHAKEN Transaction Detail Records (TDRs) are now being added as an additional data source. Each call is assessed through the Bulk Solutions model, leading to constantly refreshed view of call behavior and probability of a given number currently being used for robocalling. Active numbers are assessed by the model for behavioral attributes typically associated with robocalling including neighbor spoofing events and sudden spikes in volume (such as calls driven by spoofing). Numbers designated as Do-Not-Originate

⁴ See Robocall Mitigation – Prevention Service, Bulk Solutions, <https://www.bulkvs.com/robocall-mitigation-prevention-service>.

(DNO) numbers are also deemed to be robocalls if the DNO numbers are the calling party number. This is sourced from industry (*e.g.*, US Telecom) and directly from enterprises. The service covers both US domestic and international TNs.

The Bulk Solutions Process also provides protection from the origination of robocalls (“Robocall Protection”). Robocall Protection provides detailed reporting identifying suspected illegal robocalls and alerts if calls originate where the calling number is invalid, unallocated, or on a DNO list. If the platform detects a suspected robocalling patterns Skywire will take appropriate action which may include suspending or terminating the subscriber. The Robocall Protection solution supports a real time query to service to determine if a number originating on the network could be a robocall. Such calls can be blocked, or the terminating party can be notified via the Caller ID Name (“CNAM”). For each new instance of robocalling using the Operating Service Provider (“OSP”) TNs, an alert is sent to the OSP in near real time. This alert will result in the OSP (manually) blocking the TN and all TSPs being alerted via CNAM, through an overlay such as “ROBOCALLER”. The CNAM alerting helps address instances of spoofing of TNs that are not going through the OSP that owns the number.

The Bulk Solutions Process also provides protection against the termination of robocalls (“Robocall Mitigation”). The Robocall Mitigation solution supports a real-time query to determine if a number terminating on the network could be a robocall. This protects subscribers from calls that come from networks that cannot authoritatively attest to the end user caller (*i.e.*, all Communications Service Providers (“CSPs”) that do not have STIR/SHAKEN and all CSPs with STIR/SHAKEN but who do not have a direct and vetted end user relationship). Such calls can be blocked or the called party can be notified via CNAM.

Ownership and Management Information Information regarding Skywire’s management team can be found at: <https://skywirenetworks.com/about-us/#leadership>.