

Unite Private Networks, LLC Robocall Mitigation Plan

Unite Private Networks, LLC (“UPN”) submits this Robocall Mitigation Plan (“Plan”) pursuant to 47 C.F.R. § 64.6305. This Plan describes UPN’s efforts to mitigate illegal robocalls consistent with the FCC’s rules. UPN may modify, add, delete, or otherwise alter any part of this Plan in order to respond to changes in its business, technologies, needs, industry best practices, or any applicable law or regulations. UPN will update this Plan within ten (10) business days following the date of any changes to the Plan.

UPN’s Roles in the Call Chain

UPN operates as a voice service provider when it provides voice over internet protocol (“VoIP”) services to end-user customers.

STIR/SHAKEN Implementation Status

As a voice service provider offering VoIP service to end-user customers, UPN does not have an obligation to implement the STIR/SHAKEN Caller ID Authentication Framework. To provide VoIP service to end-user customers, UPN resells VoIP services obtained from a third-party provider White Label Communications, LLC (“White Label”). Although UPN installs and operates the fiber facilities over which UPN’s services (including but not limited to VoIP) are offered, as a reseller of VoIP services, UPN “lack[s] control over the necessary network infrastructure to implement STIR/SHAKEN.”¹ UPN therefore relies on White Label’s implementation of STIR/SHAKEN Caller ID Authentication Framework across its network, which White Label timely implemented as of June 30, 2023.

In addition to its VoIP services, UPN maintains a *de minimis* number of plain old telephone service (“POTS”) lines that are capable of transmitting voice calls but cannot initiate, maintain, carry, process, or terminate SIP calls. For these non-IP lines, UPN is eligible for a continuing extension of the STIR/SHAKEN implementation obligation pursuant to Section 64.6304(d) of the FCC’s rules.² Further and consistent with Section 64.6303(a)(2), UPN supports efforts to develop a caller ID authentication solution through its membership in Incompas.

Customer Vetting Process

UPN vets the identity of subscribers when (i) approving an application for service; (ii) provisioning of network connectivity; (iii) entering into a contract agreement; or (iv) granting the right-to-use any U.S. telephone number resources. Before onboarding customers, UPN collects information to

¹ See *Call Authentication Trust Anchor; Implementation of TRACED Act Section 6(a) – Knowledge of Customers by Entities with Access to Numbering Resources*, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3241, para. 40 (2020) (excluding from a STIR/SHAKEN implementation obligation those providers that lack control over the necessary network infrastructure); See *Call Authentication Trust Anchor*, Second Report and Order, 36 FCC Rcd 1859, para. 19 (2020).

² 47 C.F.R. § 64.6304(d).

confirm their identity including their full legal name, federal tax ID (if applicable), principal place of business, contact person, and state or country of incorporation. UPN reconfirms this information for renewing customers.

Additionally, all UPN VoIP lines are provisioned across UPN-owned or leased fiber. All VoIP lines are fully vetted and fiber is provisioned at the time of contracting. As such, it is not possible for an unknown party to place calls over UPN's VoIP solutions.

Upstream Provider Vetting Process

UPN vets its upstream providers prior to accepting their traffic through its contractual relationship with White Label and the upstream provider vetting procedures maintained by White Label (including White Label's master service agreements with its suppliers). Through its wholesale provider White Label, UPN also confirms whether the upstream provider is identified in the Robocall Mitigation Database (to the extent required).

Acceptable Use Policy and Other Robocall Mitigation Measures

UPN's Acceptable Use Policy applies to all customers using its IP services and prohibits use of such services in any way that is unlawful, harmful to or interferes with the use of UPN's network or systems, or the network of any other provider, interferes with the use or enjoyment of services received by others, or constitutes Spam/E-mail/Usenet abuse, among other prohibited uses. An example of Spam/E-mail/Usenet abuse under the Acceptable Use Policy includes sending messages that are harassing or malicious, or otherwise could reasonably be predicted to interfere with another party's quiet enjoyment of the IP services or the Internet (e.g., through language, frequency, or size). UPN may suspend or terminate a customer's IP services for failure to observe its Acceptable Use Policy. UPN's Acceptable Use Policy is available to the public on our website at: <https://uniteprivatenetworks.com/acceptable-use-policy/>.

As a reseller of VoIP services, UPN relies on other robocall mitigation measures undertaken by its wholesale provider White Label. UPN does not use any other third-party services for purposes of call analytics.

Traceback Commitment

UPN commits to respond fully, within 24 hours, to valid traceback requests made by the Industry Traceback Group (ITG), U.S. government agencies (including the FCC), U.S. law enforcement, and to cooperate with such entities in investigating and stopping illegal robocallers that use UPN's service to originate, carry, or process illegal robocalls.

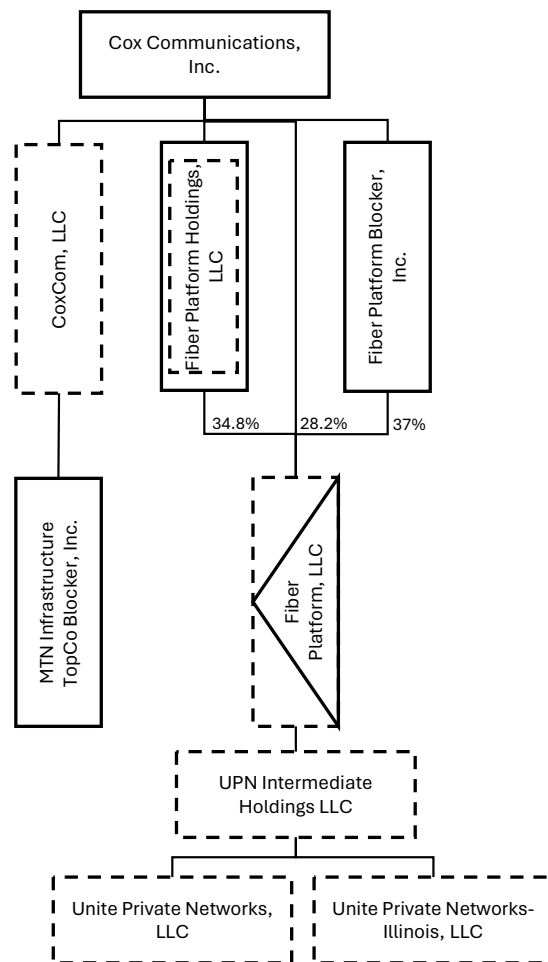
Ownership and Management

UPN's ultimate parent is Cox Enterprises, Inc. The chart attached hereto as **Exhibit A** depicts the ownership of UPN and its affiliates. Information regarding UPN's management team can be found at: <https://www.segra.com/about-segra/>.

EXHIBIT A

Ownership Structure Chart

Cox Communications, Inc.'s Segra* & UPN Ownership



**Only TopCo of Segra structure included for simplicity*

As of 12/31/2023