

CapTel Robocall Mitigation Program

CapTel is a provider of specialized communications services for individuals with hearing and speech disabilities, which are unaddressed in the FCC's robocall mitigation orders. Specifically, CapTel primarily provides a captioning service for IP CTS calls. IP CTS is used by persons with hearing loss who can speak and have some residual hearing. IP CTS allows the user to simultaneously listen to the other party and read the captions of what the other party in a telephone conversation is saying. IP CTS uses the Internet—rather than the telephone network—to provide the link and captions between the IP CTS user and the IP CTS service provider. Automated speech recognition technology, with or without the assistance of a communications assistant, transcribes the non-IP CTS user's words into captions for the IP CTS user to read. IP CTS can be used with a captioned telephone or an existing voice telephone and a computer or other web-enabled device without requiring any specialized equipment.

For the vast majority of CapTel's traffic (~96%), CapTel is not a voice service provider because it supplies only non-voice captioning data for the call and does not originate or terminate voice traffic or pass voice traffic in the call chain as an intermediate provider. A customer's voice service provider handles the voice component of the call and is responsible for STIR/SHAKEN implementation and is subject to the FCC's robocall mitigation rules.

For the remaining, very small portion of CapTel's traffic, CapTel partners with a VoIP provider, NetworkIP, to provide its customers with IP CTS that includes both voice and captioning services (referred to here as VoIP IP CTS Calls). CapTel also supports a legacy PSTN/TDM captioning service that cannot be initiated, maintained, or terminated using the Session Initiation Protocol (SIP) signaling protocol.

Caller ID Authentication

For the small portion of traffic where CapTel may be considered a voice service provider, CapTel is not currently obligated to implement STIR/SHAKEN.

VoIP IP CTS Calls

CapTel is subject to an ongoing extension under 47 C.F.R. § 64.6304(b) because it is not eligible for a Service Provider Code (SPC) token. The STI-Governance Authority requires that to obtain a token, providers must: (1) have a current form 499A on file with the FCC, (2) have been assigned an Operating Company Number (OCN), and (3) have certified with the FCC that they have implemented STIR/SHAKEN or comply with the Robocall Mitigation Program requirements that are listed in the FCC Robocall Mitigation Database. Because CapTel collects no revenue from end users, and instead is compensated from the interstate TRS Fund, CapTel is not required to, and does not have a Form 499A on file with the FCC, nor does it have an OCN. Accordingly, CapTel is not eligible for a SPC token, and it is not required to implement STIR/SHAKEN at this time.

Additionally, when a VoIP IP CTS customer makes a call, CapTel provides the IP CTS service, and it partners with NetworkIP for the voice service. CapTel does not consider itself to be a voice service provider, but out of an abundance of caution and because of the broad definition of voice service in the FCC's robocall rules, it notes that a VoIP IP CTS call technically routes from a CapTel phone to a CapTel switch before being handed over to NetworkIP. Nevertheless, NetworkIP as the partner VoIP provider, is the entity that controls the voice network.

Even though CapTel is not required to implement STIR/SHAKEN for these calls, the vast majority of VoIP IP CTS calls relayed by CapTel are authenticated under the STIR/SHAKEN framework. As set forth above, CapTel is partnered with a registered VoIP network provider, NetworkIP, which provides 10-digit DID numbers and network facilities for both inbound and outbound calls relayed by CapTel—either as the VoIP provider for certain of CapTel's customers or as the competitive local exchange carrier with which CapTel contracts for interconnection with the public switched telephone network. NetworkIP provides STIR/SHAKEN authentication on behalf of CapTel for the VoIP CapTel calls carried by NetworkIP.

For the small percentage of VoIP IP CTS traffic that currently is not routed to and authenticated by NetworkIP, CapTel is diligently evaluating whether it can find another third-party solution to ensure that those calls also are signed. Even still, as explained below, those calls are not likely to be illegal robocalls given the specialized communications service CapTel provides.

Legacy PTSN/TDM Captioning

CapTel has not implemented STIR/SHAKEN for its legacy PTSN/TDM captioning service. Pursuant to 47 C.F.R. § 64.6304(d), CapTel has an extension from any STIR/SHAKEN obligations for this service because it relies on technology that cannot initiate, maintain, carry, process, and terminate SIP calls.

Robocall Mitigation Practices

Because of the nature of CapTel's service, the incidence of illegal robocalls being carried over its network is small at best. Nevertheless, CapTel shares the FCC's desire to end the scourge of illegal robocalls and takes the following "reasonable steps" to mitigate illegal robocall traffic.

Know Your Customer

CapTel takes affirmative, effective measures to prevent customers from originating illegal calls. Indeed, due to Commission regulations applicable to CapTel's IP CTS offering, CapTel knows the identity of its users with a much higher level of certainty than traditional voice service providers. Specifically, pursuant to the FCC's rules, to use CapTel's IP CTS service, CapTel's users are required to register to receive a 10-digit number and to use CapTel's IP CTS service. The identification information collected by CapTel and required from each user as a prerequisite for such user to utilize CapTel IP CTS includes their Name, Address, Telephone Number, Date of Birth, and Last four digits of their social security number. Further, the user must, under penalty of perjury, attest to their need to register and use the CapTel service. In

addition, starting in mid-2024, all user registration information will be validated by an FCC-mandated IP CTS user registration process. Once registered for the service, users generally do not have to go through a reregistration process, if their information remains unchanged.

As permitted by FCC regulations, CapTel may suspend the use of the services if any users breach CapTel's Terms and Conditions.

Know Your Upstream Provider

As explained above, CapTel is partnered with a registered VoIP network provider, NetworkIP, to provide 10-digit DID numbers and network facilities for both inbound and outbound calls. CapTel has a longstanding relationship with NetworkIP and maintains an awareness of the nature of their business. Only Inbound calls from registered CapTel users to N11 or 911 numbers are not routed through NetworkIP. Such N11 and 911 calls are routed to Bandwidth.com for routing to the correct endpoints.

Call Analytics Systems Used to Identify Illegal Traffic

CapTel relies on its VoIP provider, NetworkIP, to monitor the network for suspicious and illegal traffic. NetworkIP's robocall mitigation program in the FCC's Robocall Mitigation Database indicates that it constantly monitors its network for suspicious calling patterns which may trigger investigation, including:

- Caller-ID numbers that generate unusually high call volumes
- Unusually high volumes of short-duration calls
- High volumes of calls with non-standard or improperly formatted Caller-IDs
- Unplanned or non-forecasted calls in bursts
- Sequentially incrementing Caller-ID or destination numbers
- High call volumes at times inconsistent with historical trends for the originator's network

Traceback Commitment

CapTel commits to respond within 24 hours to all traceback requests from the FCC, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls.