

Riverwave LLC Robocall Mitigation Plan

Riverwave LLC (“RiverWave”) provides end user interconnected VoIP services to commercial and residential customers. RiverWave utilizes [REDACTED] as its underlying voice services provider. RiverWave relies in part on [REDACTED]’s processes, procedures, and systems to mitigate illegal robocalling.

Knowledge of Upstream Providers

RiverWave contracts with [REDACTED] as its upstream VoIP provider. RiverWave has insight into its upstream provider’s policies and procedures related to identifying and blocking unlawful robocall traffic through RiverWave’s review of its provider’s robocall mitigation plans. RiverWave confirms, through [REDACTED], that all upstream providers from which it receives traffic are listed in the FCC’s Robocall Mitigation Database.

STIR/SHAKEN

On behalf of RiverWave, [REDACTED] has implemented STIR/SHAKEN on its network where all of RiverWave’s voice traffic originates. [REDACTED] has also adopted its own robocall mitigation plan to limit the potential for unlawful calls from or on its network.

Robocall Mitigation Program/Analytics

On behalf of RiverWave, [REDACTED] has implemented its own call analytics to identify unlawful traffic originated by its retail customers and the end users of its wholesale customers’ services. These call analytics can detect call patterns that indicate robocall activity, including, but not necessarily limited to, an unusually large number of calls from the same number, an excessive number of short duration calls, and calls that stop attempting to connect after a single ring. The call analytics also can detect where the calling number is invalid, unallocated, or on ITG’s Do Not Originate (“DNO”) list. If the call analytics detect any of the above-described issues, an internal report is generated that summarizes the issues presented and the customer responsible for the underlying calls.

In the event that the analytics report indicates potential illegal robocall activity, RiverWave works with [REDACTED] to take action commensurate with the severity of the customer’s offense, including, but not limited to, providing the customer with a warning or terminating the customer’s service and/or reporting the misconduct to the appropriate authorities.

Knowledge of Customers

RiverWave vets the identity of its customers prior to entering a contract for VoIP services. As part of this vetting process, RiverWave collects the customer’s name/business name and address, physical location, and contact information and compares it to publicly available sources to verify

matching data. RiverWave will not provide service if a new customer's identification cannot be verified.

RiverWave's terms and conditions are accepted by all new customers and updated from time to time as needed. These terms and conditions explicitly prohibit illegal robocalling behavior. To the extent a customer is found to have violated its contractual obligations, RiverWave reserves the right to disconnect service.

Traceback

RiverWave, through and in concert with its upstream provider, is committed to responding fully and within 24 hours to all traceback requests made by ITG, law enforcement authorities, and government agencies to investigate and address suspected unlawful robocalls originated or passed to RiverWave. RiverWave, through its upstream provider, is committed to fully complying with the Commission's robocall blocking requirements and confirms that it will block all calls and provider traffic that: (1) are identified in any public notice or order released by the FCC; (2) are substantially similar to the types of traffic identified in any public notice or order released by the Commission; or (3) include a caller ID number or name that is on DNO list issued by ITG. RiverWave, through its upstream provider, also blocks the traffic of all foreign providers and gateway providers that have not registered in the Robocall Mitigation Database.