

Sprinklr, Inc.

Robocall Mitigation Plan

Sprinklr, Inc. (“Sprinklr”) offers Voice over Internet Protocol (“VoIP”) calling features for use with certain of its customer experience services. These features are provided with the support of Sprinklr’s carrier partners, who perform first-party STIR/SHAKEN authentication on all calls originated on behalf of Sprinklr end-users. While Sprinklr relies on the robocall mitigation practices of its carrier partners, Sprinklr has adopted this robocall mitigation plan to further limit the potential for the origination of unlawful robocalls by its customers that may be transmitted by its carrier partners and downstream providers.

Know Your Customer Policies and Controls

Customer Validation: Sprinklr only provides calling services to enterprise customers following a vetting process. Sprinklr validates prospective customer’s identity before entering into a service agreement with the customer. As part of this process, the customer must provide their legal name and address, contact information, business location (if different from their correspondence address) and federal tax ID. Sprinklr maintains this information on all customers. If the customer’s identity cannot be verified based on the initial information provided, the customer may be required to provide additional information. This information enables Sprinklr to ensure the identity of a potential customer has been properly validated prior to provisioning calling services.

Contractual Obligations: Sprinklr requires customers to comply with an Acceptable Use Policy (“AUP”) that prohibits a customer’s use of its services for any unlawful purpose, including, but not limited to, violations of laws including those regulating unsolicited or unwanted communications and telemarketing. To the extent a customer is found to have violated Sprinklr’s AUP for the reasons noted previously or any other reason, Sprinklr will take action commensurate with the severity of the customer’s offense, including, but not limited to, providing the customer with a warning, suspending the customer’s service without notice, or terminating the service agreement with the customer.

In addition to Sprinklr’s AUP, Sprinklr requires customers to comply with its carrier partners’ contractual terms and acceptable use policies prohibiting unlawful or fraudulent use of the calling services.

Customer Education: Sprinklr is also committed to providing its customers with education regarding responsible outbound calling and provides said customers with guidelines to ensure they are engaging in outbound calling in a responsible and legally compliant manner.

Use of Call Analytics to Identify and Block Unlawful Traffic

Sprinklr relies on both its own analytics as well as its downstream carrier partners' use of call analytics systems to identify and block unlawful robocall traffic as set forth in their robocall mitigation plans on file with the FCC.

Sprinklr uses different methods to track trends related to the use of its services. These include monitoring customer usage and calling patterns. Sprinklr applies per-account concurrent call limits, which restrict a customer's ability to place large numbers of automated calls.

Sprinklr's carrier partners have reported that the call analytics they employ for Sprinklr's traffic can also 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, as well as calling numbers that are invalid, unallocated, or on the Industry Traceback Group's ("ITG") Do Not Originate ("DNO") list. If Sprinklr receives a report or alert from any downstream carrier partner of suspected unlawful robocall traffic originated by a Sprinklr customer, Sprinklr will conduct an investigation. To the extent a customer is found to have violated its contractual agreement with Sprinklr, Sprinklr will 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 without notice.

Knowledge of Upstream Providers

Sprinklr's service is not configured to accept traffic originated by third parties; therefore, Sprinklr does not serve any upstream providers.

Cooperation with the Traceback Group, Law Enforcement and Government Agencies

Sprinklr 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 by Sprinklr's end user customers.

Sprinklr is also committed to cooperate with its carrier partners on traceback requests and to fully comply with the Commission's robocall blocking requirements. Sprinklr understands that its carrier partners 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.