

Robocall Mitigation Programme (RMP) V3.0

This document updates our RMP efforts using best practices gleaned from Industry sources

Robocall definition used:

We rely on three FTC sources, one FCC and one DOJ source from Dec 2021 to define robocalls as broadcast of pre-recorded messages to landlines or automated calls to mobile phones. The sources are:

1 National Do Not Call Registry FAQs

“a [robocall](#) — a call that plays a recorded message”

<https://www.consumer.ftc.gov/articles/national-do-not-call-registry-faqs>

2 Robocalls

“If you answer the phone and hear a recorded message instead of a live person, it's a robocall.”

<https://www.consumer.ftc.gov/articles/robocalls>

3 Robocalls

“..prerecorded telemarketing calls, commonly known as robocalls”

<https://www.ftc.gov/news-events/media-resources/do-not-call-registry/robocalls>

4 Robocalls

“for a landline, if the call leaves a prerecorded or artificial voice message on the landline phone, that's a robocall as long as it's telemarketing.on wireless phones, calls to wireless phones, it's a robocall if it leaves those types of messages, prerecorded or artificial voice message, or if the call is made with what we call an autodialer which is simply equipment that can make a call really quickly to multiple numbers.”

<https://www.fcc.gov/news-events/podcast/robocalls>

5 Case 2:20-cv-00474-BMC

“ "Robocall" means a call made through an automated process that places large volumes of telephone calls over the internet in order to deliver recorded messages, in contrast to calls placed one at a time by a live person.”

<https://www.justice.gov/opa/press-release/file/1240031/download>

Illegal Robocall mitigation

We use heuristics to detect illegal robo-calling patterns such as short but intense calling period, calls of similar length, and other heuristics developed over time. We attempt to verify each calling number through a mix of manual and automated processes, and if that fails, approach the customer or block traffic for resolution.

Binning of traffic: Customers are binned by traffic into call center or retail and business. This is done by a combination of customer declaration as well as traffic analytics. In cases where we can distinguish such traffic, call center traffic is further divided into auto and manual dial.

Vetting of ANI/CallerID: Outbound callerIDs will be analysed daily based on traffic volume and investigated for suspicious calling patterns.

Similarity analysis: Customers once blocked will be subject to similarity analysis with other usernames to ensure they do not reappear under other pseudonyms.

Industry cooperation

We fully cooperate in industry traceback efforts and law enforcement requests. We will respond fully, within 24 hours, to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and will cooperate with such entities in investigating and stopping illegal robocallers that use our service to originate, carry, or process illegal robocalls.

Know Your Customers (KYC): We will confirm the identity of all customers with following information. New customers will be asked at start of service and existing customers on a periodic basis.

1. Description of calling process
2. Tax payer number if requiring more than a single channel account.
3. For OSPs, a copy of their OSP registration number
4. List of DBA and brand names
5. Billing address
6. Physical calling address or calling addresses if distributed.
7. Email address of person paying bills
8. Email address should be of a custom domain or must be from their web site domain
9. website address, including websites used for the calling process

Third-Party Analytics Vendors

We do not currently use any third-party analytics vendors for our robocall mitigation efforts. All traffic analysis and mitigation actions are performed internally using proprietary tools and heuristics. Should this change in the future, we will update the program and upload.