

1. Robocall Mitigation Plan

1.1. Introduction

NTT Cloud Communications U.S. Inc. has worked with its PSTN termination partners to implement SHAKEN/STIR signing of outbound PSTN calls. Additionally, NTT Cloud Communications inc. uses a suite of fraud and robocall protection tooling based on software provided by our software partner.

NTT Cloud Communications U.S. Inc. operates a 24/7 telephony fraud monitoring team who receive real-time alerts from the fraud monitoring systems, and investigate and intervene as needed, including by blocking outbound calls if this is determined to be necessary.

The Robocall and more general fraud mitigation methods used are summarised below.

1.2. Call Analytics/Robocall Monitoring

All outbound PSTN calls from NTT PSTN-enabled voice platforms are processed by our outbound routing proxies which implement detection, reporting and protection for Robocalls.

The system monitors all call attempts originating from the same Calling Number in each 1-hour period and reports daily and hourly on Calling Numbers with a high volume of originating calls.

Events generated are reviewed daily by NTT's fraud monitoring team, and where the call patterns are potentially suspicious, they will take steps to validate that (a) the originating number is being legitimately used and (b) the calls are consistent with legitimate use of PSTN calling.

Customers will be notified of the suspicious activity to ensure that they are in compliance with regulatory requirements and if traffic continues, we reserve the right to terminate the service according to our AUP guidelines.

1.3. DNO Blocking

NTT Cloud Communications U.S. Inc. has implemented systematic DNO ("do not originate") blocking on its network, based on the Industry Traceback Group's DNO registry (<https://tracebacks.org/dno-registry/>).

This is implemented on both inbound and outbound call routing elements in the network, ensuring that:

- Calls entering NTT Cloud Communications U.S. Inc.'s network where the originating number is listed in the registry are blocked and not delivered to subscribers; and
- Calls originated by subscribers on NTT Cloud Communications U.S. Inc.'s network, where the originating number is listed in the registry, are blocked and not terminated to the PSTN.

1.4. Know Your Customer

NTT Cloud Communications exercises due diligence with our upstream customers to help ensure that the type of traffic generated is in compliance with regulatory requirements and that relevant information regarding the end customers is known so that NTT Cloud Communications U.S. Inc. is not used to transit illegal traffic and/or be able to remediate if identified.

1.5. Traceback Requests

NTT Cloud Communications U.S. Inc. is committed to responding to all traceback requests from the various legal, regulatory and industry authorities in a reasonable time.

1.6. Principles and Parent Companies

Pursuant to paragraph 46 of the Sixth Caller ID Authentication Report and Order (FCC 23-18 adopted on March 16, 2023), NTT Cloud communications US Inc. is required to provide information regarding our principals, affiliates, subsidiaries, and parent companies.

- NTT Cloud communications US Inc. is 100 % owned by NTT Cloud Communications SAS (company registered in France).
- NTT Cloud Communications SAS is owned up to 100 % by NTT Cloud Communications International Holdings SAS (company registered in France).
- NTT Cloud Communications International Holdings SAS is owned up to 100% by NTT Limited (company incorporated in the United Kingdom)
- NTT Limited is a wholly owned subsidiary of NTT Data, Inc. (Japanese corporation)
- NTT Data, Inc. is owned by Nippon Telegraph and Telephone Corporation, a Japanese listed company on the Tokyo Stock Exchange up to 45% and NTT Data Group Corporation a company also listed on the Tokyo Stock Exchange, up to 55%."