

Robocall Mitigation Plan

Business Information

Dixa ApS
Artillerivej 86, st. tv.
Denmark

Contact Information

Søren Dam Hansen
Sr. Director, Legal & Compliance
+4589886260
legal@dixa.com

Overview

In the Commission's release, *In the Matter of Call Authentication Trust Anchor, Sixth Report and Order and Further Notice of Proposed Rulemaking*, WC Docket No. 17-97 (rel. March 17, 2023) ("R&O") it is stated that all voice service providers ("VSPs") must file robocall mitigation plans ("RMPs") that, among other things, outlines "reasonable steps" taken to avoid originating illegal robocalls.

In addition to the "reasonable steps," the FCC requires that a RMP include:

- "know your customer" procedures;
- "know your upstream provider";
- ownership information;
- a description of any call analytics system used to identify and block illegal traffic; and
- whether a third-party vendor is used and if so, the name of the vendor.

The FCC previously stated that a RMP is sufficient if the detailed practices in the plan can reasonably be expected to significantly reduce the origination of illegal robocalls and the VSP complies with the practices it describes in its filing.

Purpose

Dixa ApS ("Dixa") is a small VSP dedicated to stopping illegal calls from originating in our network and monitoring the calls traversing our network. Because Dixa lacks control of the infrastructure necessary to implement STIR/SHAKEN, it is not required to be STIR/SHAKEN compliant. In compliance with the R&O, Dixa submits this RMP and certification.

Know Your Customer ("KYC")

The accurate identification of a subscriber in the STIR/SHAKEN ecosystem is tied to a telephone number-based caller identity associated with that subscriber. A subscriber is an entity that has a business relationship with Dixa in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

Dixa vets its subscribers by collecting their names, addresses, billing information, and VAT numbers. If a US number user wishes the ability to send SMS, we will run a KYC request as mandated by the reselling carrier.

Know Your Upstream Providers

In accordance with the Commission's directive in *Advanced Methods to Target and Eliminate Unlawful Robocalls Call Authentication Trust Anchor, Seventh Report and Order In CG Docket 17-59 and WC Docket 17-97, Eighth Further Notice of Proposed Rulemaking In CG Docket 17-59, and Third Notice of Inquiry in CG Docket 17-59* (Rel. May 19, 2023) ¶¶ 49-51, Dixa provides the following information concerning its upstream voice service carriers.

Twilio Ireland Limited
70 Sir John Rogerson's Quay
Dublin 2, D02 R296, Ireland
Erica Soh
esoh@twilio.com

Bandwidth, Inc.
900 Main Campus Drive
Suite 100
Raleigh, NC 27606
Dean Boulden
dboulden@bandwidth.com

DIDWW Ireland Limited
11 The Haven,
Malahide, Co. Dublin, Ireland,
Alicija Raciene,
alicia.r@didww.com

Avoxi, Inc.
300 Galleria Parkway
Suite 610
Atlanta, GA 30339
Ken Barber
ken.barber@avoxi.com

Voxbone SA
Avenue Louise 489
1050 Brussels
Belgium
dboulden@bandwidth.com

Dixa and its upstream providers work together to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Acceptable Use Policy ("AUP")

Dixa maintains an Acceptable Use conditions that subscribers must accept before being permitted to use Dixa's network. See <https://www.dixa.com/legal/tos/>.

Analytics for Monitoring Traffic

Dixa works with its upstream carriers to analyze high-volume voice traffic to identify and monitor patterns consistent with robocalls. Our upstream carriers' systems alerts them to calling patterns with unusual spikes, traffic patterns, and related matters. If a calling pattern is detected that is consistent with illegal robocalls, Dixa and its upstream providers will identify the party that is using the carrier's network to transmit those calls and will take appropriate action. Taking appropriate action may include, but is not limited to, initiating a traceback investigation, verifying that the originating subscriber owns or is authorized to use the Caller ID number, and suspending or terminating the party's ability to originate calls on our network.

Twilio, Bandwidth, Voxbone, Avoxi and DIDWW are third party vendors involved in deploying Dixa's analytics.

Investigate Suspicious Activity

Suspicious activities are typically raised by Dixa's upstream providers. Dixa cooperates fully in any and all investigations involving suspicious calling patterns and other instances that indicate illegal robocall patterns.

Blocking

Dixa works with its upstream carriers to abide any Do Not Originate requests it receives from the Industry Traceback Group ("ITG"). Dixa will cooperate with Investigative Bodies (provide a single point of contact) to address traceback requests from law enforcement and regulatory entities such as state attorneys general, the FCC, and/or ITG; as well as documenting requests & actions taken in response thereto. Dixa certifies that it will respond to all traceback requests within 24 hours.

Plan Updates

This plan and industry best practices must evolve to response to the dynamic nature of mitigating illegal robocalling. Dixa will monitor industry best practices and continuously improve our internal processes to ensure this plan, and our system adapt to this ever-changing issue.

In the event of any material change to this plan, Dixa will republish it to employees, consultants and contractors and file such an update to the FCC Robocall Mitigation Database within ten (10) days of such update.

Certification of Soren Dam Hansen

I, Soren Dam Hansen, Sr. Director, Legal & Compliance of Dixa ApS ("Dixa") do hereby certify, under penalty of perjury, the following:

- a. Dixa is not required to implement STIR/SHAKEN, due to its lack of control over the necessary infrastructure.
- b. Dixa's business name and primary address are as follows:

Dixa ApS
Artillerivej 86, st. tv.
Denmark
- c. Dixa has no other business name.
- d. Dixa has not previously used any other business name.
- e. The name, title, department, business address, telephone number, and email address of the individual responsible for addressing robocall-related issues are listed in the above robocall mitigation plan.
- f. The following entities have more than 10% ownership in Dixa: General Atlantic DX B.V., Fosselius Invest ApS, Project A Ventures II GmbH & Co. KG, SEED Capital Denmark III K/S; Dixa Inc, Dixa Ltd, Miuros SAS, Dixa GmbH, Dixa Australia Holding Pty Ltd, Elevio Pty Ltd are Dixa's affiliates or subsidiaries.
- g. Dixa's role in the call chain is that of a voice service provider with no STIR/SHAKEN implementation obligation.
- h. Dixa is not prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- i. Dixa has not been subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- j. Dixa is not required to, and does not have, an Operator Code Number.

Søren Dam Hansen

Soren Dam Hansen