

Robocall Mitigation Plan for Dropbox

Last updated February 28, 2026

Overview of the Dropbox Fax Service

Dropbox, Inc. and Dropbox International Unlimited Company (collectively, “Dropbox”) provide the Dropbox Fax service, an Internet-based information service through which customers send and receive fax messages via the Dropbox Fax web application (web app) or Application Programming Interface (API).

Dropbox contracts with a small number of third-party vendors to provide the Dropbox Fax service. For outbound faxing, Dropbox contracts with Concord Technologies Corporation (“Concord”) and NG Communications bvba (“NGC”), which send outbound faxes placed by Dropbox Fax customers via the Dropbox Fax web app or API. When a Dropbox Fax customer requests to send an outbound fax, Dropbox makes a call to either Concord’s or NGC’s API. As part of the API call, Dropbox provides the customer’s file and the recipient’s fax number (or email address) to Concord and NGC. Concord and NGC process and ultimately send the outbound faxes via their networks.

For inbound faxing, Dropbox engages Voxbone S.A. (“Voxbone”). When a fax number that belongs to a Dropbox Fax customer receives a fax, Dropbox receives an API call from Voxbone that includes the fax file and the recipient fax number. Dropbox then matches the fax number to the correct customer account and places the file in their account. Voxbone also provides fax numbers to Dropbox Fax customers.

STIR/SHAKEN Exemption

Under 47 CFR § 64.6301(a), only voice service providers that transmit or receive “SIP calls” must implement STIR/SHAKEN. *See also* 47 CFR § 64.6304(d) (providing a continuing extension for technologies that “cannot initiate, maintain, carry, process, and terminate SIP calls”). Dropbox does not transmit or receive faxes using the SIP signaling protocol, and STIR/SHAKEN, at present, only works with SIP technologies. *See In re In the Matter of Targeting and Eliminating Unlawful Text Messages*, Report and Order and Further Notice of Proposed Rulemaking, FCC 23-21, para. 37 (2023). In addition, as an Internet-based information service, Dropbox does not own or operate telecommunications equipment or resell any telecommunications services. Further, Dropbox does not control the network infrastructure and facilities necessary to implement the STIR/SHAKEN authentication framework. *See, e.g., Second Caller ID Authentication Report and Order*, 36 FCC Rcd 1859, 1868, para. 19 (2020) (citing *First Caller ID Authentication Report and Order*, 35 FCC Rcd 3241, 3260, para. 40 (2020)). As a result, Dropbox is exempt from implementing STIR/SHAKEN on its network.

Robocall Mitigation Plan

Dropbox has taken the following steps to prevent the origination of illegal robocalls:

- Dropbox has procedures in place to confirm the identity of new and renewing Dropbox Fax customers. For example, Dropbox collects certain customer information, including subscriber names, email addresses, and billing information. Dropbox also publishes the Dropbox Sign Terms of Service (TOS), Service Specific Terms (SST), and Acceptable Use Policy (AUP), which govern access to and use of the Dropbox Fax service, on its website. The SST requires Dropbox Fax customers to provide Dropbox with accurate and up-to-date information, including name, billing information, and national ID number (where applicable). Dropbox Fax customers must also provide Dropbox with true, accurate, and up-to-date information in connection with any request to port in or port out numbers to or from the Dropbox Fax service.
- The TOS and AUP prohibit, among other things, the use of the Dropbox Fax service to transmit unsolicited faxes or spam, or for any other unlawful purpose. Dropbox may suspend or terminate access to the Dropbox Fax service for violations of the TOS or AUP.
- To combat platform abuse, including unlawful robocall campaigns, Dropbox enforces rate limits on the number of outbound faxes certain customers can send .

Dropbox has implemented “Know Your Customer” policies:

- Dropbox contracts with a limited number of upstream and downstream providers (Concord, NGC, and Voxbone) and has a point of contact for robocall mitigation matters at each provider.
- As noted above, Dropbox collects certain customer information, including subscriber names, email addresses, and billing information.

Dropbox also commits to:

- Respond to traceback requests from the Federal Communications Committee (FCC), civil and criminal law enforcement, and the FCC-designated industry traceback consortium within 24 hours;
- Cooperate with the aforementioned entities in investigating unlawful robocalls; and,
- Block any unlawful robocalls if notified to do so by the FCC.

Dropbox certifies that it is not prohibited from filing in the Robocall Mitigation Database. Dropbox also certifies that it is not and has not been subject to an FCC, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.

Dropbox does not have an Operating Company Number (OCN).

If there is a material change to this plan, Dropbox will file an updated Robocall Mitigation Plan with the FCC’s Robocall Mitigation Database.