



Robocall Mitigation Plan

February 2026

PURPOSE

As a part of the telephone ecosystem, Dialpad has an interest in and legal obligation to safeguard the efficient and secure operation of the nation's phone system. The following Robocall Mitigation Plan provides a non-exhaustive overview of the technical and operational measures that Dialpad employs to reduce and deter the use of its network for unlawful robocalls.

MITIGATION MEASURES

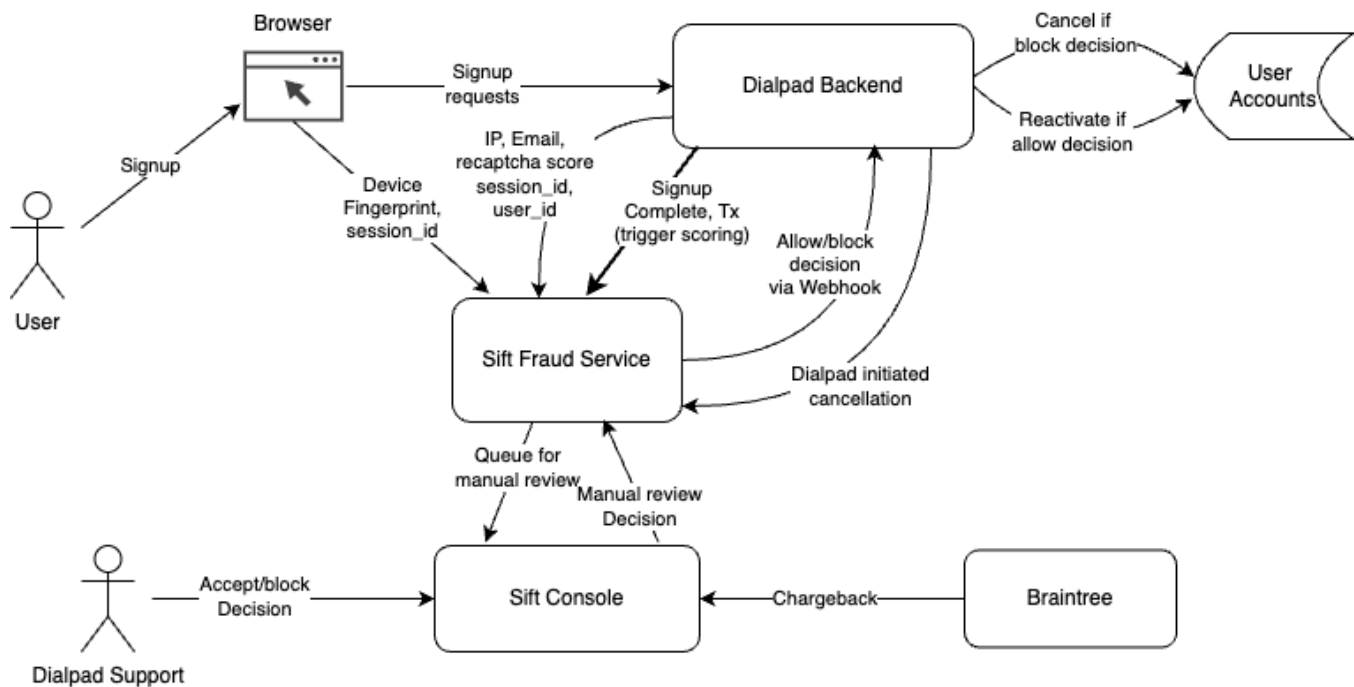
1. CUSTOMER SIGNUP

Robocall mitigation starts at signup. Dialpad employs layers of verification measures to ensure that users of its service are legitimate and do not pose an unacceptable risk of robocalls or other unlawful activities, including:

Sift Fraud Prevention Platform

Through the Sift platform, Dialpad collects signals from the customer journey including device, browser, IP intelligence, mobile verification phone number, billing and payment information, Google reCAPTCHA results, and transaction processing results from payment processor Braintree. These signals drive a machine-learning-based risk scoring that is trained on user signals, fraud data collected from a global network, and manually labeled training data to distinguish between fraudulent and legitimate activities.

If the Sift score indicates an account exceeds the risk threshold, Dialpad will reject the registration pending ID verification through Stripe.



Dialpad's second-step verification system allows immediate diversion of potentially risk signups to a verification flow that can differentiate customers from bad actors.

Domain & Company Presence Review

In addition to the dynamic measures discussed above, Dialpad maintains a known list of fraudulent email domains. When a user signs up or a team member is added, Dialpad checks their domain against these known domains and blocks where required. Signups from disposable email domains are not permitted (Static Domain Blocklist).

When a user signs up or a team member is added, Dialpad checks their domain against a custom list of fraudulent email domains called FraudDomains. Dialpad adds to FraudDomains when an office has been canceled for fraud, and prevents activation/reactivation from domains flagged for fraud.

Dialpad filters fraudulent accounts through mobile verification. Dialpad requires users to receive a phone call or text, and then sign up using a PIN code.

Known Fraud Card Denylisting

Dialpad maintains a list of payment cards associated with prior canceled fraud accounts. In addition, Dialpad's payment processor Braintree also validates credit cards for risk against its own list of known fraud accounts and bin blocks for high-fraud banks. Payments made by gift, prepaid, and temporary cards are strictly prohibited.



2. ACCESS

IP Access

Dialpad uses Google Cloud Armor, which prevents access from certain high-risk IP ranges and updates in real time. In addition, we have internal IP restrictions for operation (e.g. login from embargoed and high-risk countries). Small accounts are immediately canceled if they're accessed from denylist/high-risk countries.

Account Access

As of 2025, Dialpad enforces SSO or MFA (email or SMS) on login to all new and existing accounts that have outbound calling/messaging capabilities. This helps our users maintain control of their accounts and reduces the potential for unauthorized calls and messages.

3. RATE LIMITING

Dialpad's rate limiting includes setting caps on the rate, daily volume, and total number of calls and texts for trial and new paid accounts. Any young paid accounts exceeding these limits are suspended.

4. ANALYTICS & MONITORING

Dialpad monitors call volume across its network and examines patterns that may be associated with fraud or robocall usage.

5. INCIDENT RESPONSE

We participate in and act on reports from industry partners including the USTA Industry Traceback Group (ITG), Inteliquent, and Bandwidth. Reports of AUP violations, including robocalls, are reviewed and responded to within 24 hours, as prescribed by our agreement with the carriers. Reports include those generated through automated internal or external analytics, as well as reports from individual users and customers. Dialpad's contracts with its end users and upstream providers include AUP requirements subject to enforcement via automated analytics and manual review.

6. THIRD PARTY ANALYTICS

Dialpad does not use third party analytics vendors for outbound telephony; however as noted above Dialpad does use the Sift platform (sift.com) for customer validation at account creation and for account takeover detection/remediation, both of which are factors in robocall mitigation.

PRINCIPALS, AFFILIATES, SUBSIDIARIES, & PARENT COMPANIES



PRINCIPALS

Craig Walker, CEO

Brian Peterson, CTO

Vincent Paquet, CPO

Jim Blum, COO

Colby Nish, CRO

Atit Shah, CSO

Tasha Liniger, CHRO

Joe Faber, GC

AFFILIATES

No affiliates.

SUBSIDIARIES

Dialpad Japan K.K. (Japan)

Dialpad Canada, Inc. (Canada)

Dialpad APAC PTE. LTD. (Singapore)

Dialpad Services Private Limited (India)

Highfive Technologies, Inc. (Delaware)

Dialpad France S.A.S. (France)

Dialpad S.A.S. (Ecuador)

Koopid, Inc. (Delaware)

Dialpad Philippines Inc.

Dialpad, Inc. (Norway branch office)

Surfboard Technology Limited (UK)

Dialpad Australia Pty. Ltd. (Australia)



Dialpad UK Limited (United Kingdom)

Koopid India Pvt Ltd (India)

PARENT COMPANIES

No parent companies.

REVISION HISTORY

Description	Revision Date
Initial filing	February 26, 2024
Update adding information regarding principals, affiliates, subsidiaries, and parent companies, as well as third party analytics vendors.	November 22, 2024
Added additional information on functioning of the Sift Fraud Prevention Platform, added MFA requirement, and updated Principals	February 20, 2026