

ResiDesk Inc. robocall mitigation plan

Date: June 23, 2026

Business information

ResiDesk Inc. is a software company that provides property-management, leasing, and resident communication technology.

FCC Registration Number: 0038571485

Business address: 222 Broadway, Suite 1903, New York, NY 10038

Contact information

Arjun Kannan
Co-founder
arjun@theresidesk.com
+1 720-326-4767

Providers referenced in this plan

Bandwidth Inc. is ResiDesk's upstream voice service provider. For the calls covered by this plan, Bandwidth supplies the telephone numbers, PSTN connectivity, and carrier-level voice services that connect calls to and from the public telephone network.

LiveKit is an example of a SIP provider that ResiDesk may use inside its software to route, bridge, or handle calls after Bandwidth has supplied the telephone number and PSTN connectivity. ResiDesk may use LiveKit or a successor SIP provider selected by ResiDesk for these application-level functions.

Overview

ResiDesk submits this robocall mitigation plan for inclusion in the FCC Robocall Mitigation Database. This plan describes the limited voice functionality available through ResiDesk's software and the steps ResiDesk takes to reduce the risk that its services are used for illegal robocalls, spoofing, or other unlawful calling activity.

ResiDesk uses Bandwidth-provisioned telephone numbers and Bandwidth-provided PSTN connectivity for the public-telephone-network portion of the covered calls. ResiDesk may also use

SIP providers selected by ResiDesk, including LiveKit or a successor provider, to receive, route, bridge, or handle calls within approved ResiDesk application workflows.

The covered use case is limited to leasing and resident communication workflows for property-management customers. The service is primarily used for inbound calls placed to ResiDesk-assigned Bandwidth numbers. ResiDesk may support limited outbound leasing or resident follow-up calls when those calls are part of an approved ResiDesk workflow, such as returning a prospect or resident inquiry, scheduling leasing follow-up, or following up on a resident-service request.

ResiDesk does not offer a general-purpose outbound dialing product. ResiDesk does not provide bulk calling, campaign dialing, predictive dialing, robocalling, SIP trunk resale, or unsolicited outbound calling. ResiDesk does not operate as a gateway provider or foreign voice service provider. ResiDesk does not have an Operating Company Number.

STIR/SHAKEN implementation status

ResiDesk is filing as a domestic voice service provider without a direct STIR/SHAKEN implementation obligation. ResiDesk does not operate the carrier network infrastructure needed to sign calls with STIR/SHAKEN. ResiDesk does not currently have its own Service Provider Code token, STIR/SHAKEN certificate, or call-signing capability.

To the extent STIR/SHAKEN authentication, PSTN interconnection, number provisioning, network-level traceback support, traffic analytics, or network-level blocking applies to calls involving ResiDesk-assigned Bandwidth numbers, ResiDesk relies on Bandwidth for those carrier-level functions. If a permitted outbound follow-up call is initiated through a ResiDesk workflow, PSTN termination and any applicable network-level call authentication are handled by Bandwidth or another approved upstream voice provider.

ResiDesk will reassess this filing before enabling any materially broader outbound calling functionality, direct PSTN interconnection, customer-controlled outbound call origination outside approved workflows, or any other change that would affect ResiDesk's STIR/SHAKEN status.

Covered traffic and prohibited uses

ResiDesk limits voice functionality to approved software workflows for legitimate property-management, leasing, and resident-service purposes. Customer access is tied to ResiDesk accounts, approved workflows, assigned numbers, and customer configurations.

ResiDesk prohibits use of its systems for illegal robocalling, spoofing, fraudulent calling, bulk campaign dialing, predictive dialing, unsolicited outbound calling, or calls placed with unauthorized caller ID information. ResiDesk also prohibits use of its systems as a substitute SIP trunking or outbound telephony resale service.

If ResiDesk later expands the product to support broader outbound PSTN calling, campaign dialing, customer-controlled origination outside approved workflows, or another materially different voice use case, ResiDesk will review whether this plan and its RMD filing need to be updated before that functionality is enabled.

Know-your-customer practices

For customers with access to voice workflows, ResiDesk maintains records that identify the customer account, business contact, authorized users, configured workflows, assigned telephone numbers, and relevant property or account configuration. ResiDesk's customers are not anonymous general telephony users.

ResiDesk may review customer identity, account information, billing information, property-management context, number assignment, and workflow configuration before or during activation of voice functionality. ResiDesk may require additional information or restrict functionality if account information, usage, or a requested workflow raises compliance or abuse concerns.

Based on records reasonably available to ResiDesk, ResiDesk can identify the customer, account, workflow, or user associated with relevant call-routing activity. ResiDesk may suspend or disable affected accounts, users, integrations, phone-number workflows, or call-routing configurations if misuse is suspected.

Upstream provider and vendor coordination

Bandwidth is ResiDesk's current upstream voice provider for telephone numbers, PSTN connectivity, and carrier-level voice services associated with this filing. ResiDesk may use SIP providers selected by ResiDesk, including LiveKit or a successor provider, for application-level call routing, bridging, and AI-assisted call handling in approved ResiDesk workflows.

ResiDesk will maintain records of its upstream voice and SIP providers. ResiDesk will cooperate with Bandwidth, its SIP provider, and any other relevant provider in investigating suspected illegal robocalling, spoofing, misuse, traceback requests, complaints, or other abuse.

ResiDesk will not intentionally route covered voice traffic through an upstream voice provider that ResiDesk understands to be prohibited from accepting, carrying, or processing such traffic under applicable FCC rules.

Monitoring and analytics

ResiDesk's current voice use is limited and workflow based. It does not include bulk outbound calling or campaign dialing. ResiDesk does not currently operate its own carrier-level robocall

analytics system and does not use a separate outside robocall analytics vendor for outbound telephony.

ResiDesk relies on Bandwidth for carrier-level traffic analytics and network-level blocking where applicable. At the application layer, ResiDesk may review available logs, workflow configuration, access records, call-routing activity, complaints, upstream-provider reports, and customer or user behavior.

If ResiDesk becomes aware of a complaint, traceback request, unusual available usage data, upstream-provider report, or other indicator of suspected illegal robocalling or spoofing, ResiDesk will investigate and take action within its control.

Traceback and regulatory cooperation

ResiDesk will cooperate with traceback requests, FCC inquiries, law-enforcement inquiries, Industry Traceback Group requests, and upstream-provider investigations related to suspected illegal robocalling or spoofing.

ResiDesk will use commercially reasonable efforts to respond fully and within 24 hours to traceback requests from the Commission, law enforcement, and the Industry Traceback Group to the extent the request relates to records reasonably available to ResiDesk. ResiDesk will preserve relevant records reasonably available to it and coordinate with Bandwidth and other relevant providers as needed.

Blocking, suspension, and remediation

If ResiDesk determines that its systems are being misused for illegal robocalling, spoofing, unauthorized outbound calling, campaign dialing, or other prohibited conduct, ResiDesk may take remedial action. Available actions include disabling affected workflows, disabling call routing, suspending users or customer accounts, preserving relevant records, notifying upstream providers, cooperating with traceback or law-enforcement requests, and terminating access where appropriate.

ResiDesk may also honor carrier-imposed restrictions or blocking requirements when needed to prevent suspected unlawful traffic from continuing.

Regulatory history

To ResiDesk's knowledge, during the prior two years, ResiDesk and any commonly owned or controlled entities have not been subject to a formal FCC, law-enforcement, or regulatory agency action or investigation with findings of actual or suspected wrongdoing related to illegal robocalls, spoofing, or deficient Robocall Mitigation Database filings.

Training and internal ownership

ResiDesk will maintain internal ownership for robocall mitigation, traceback response, and upstream-provider coordination. Personnel involved in activating or supporting voice workflows will be instructed on the limits in this plan, including the restriction against bulk calling, campaign dialing, predictive dialing, unlawful robocalling, spoofing, and unsolicited outbound calling.

Plan updates

ResiDesk will review this plan if its voice functionality, upstream providers, call flows, or provider classification materially changes.

ResiDesk will update its RMD filing within 10 business days if required information changes and will complete any required annual recertification by the applicable FCC deadline.