



Robocall Mitigation Plan

Version	1.0.0
Last Updated	2025-01-31
Contact Information	fidelius-cores@bendingspoons.com

Table of Contents

[Table of Contents](#)

[Overview](#)

[Terms of Service](#)

[Suspicious Activity Investigations](#)

[Public Safety](#)

[No Former Formal Actions or Investigations](#)

[Plan Updates](#)

[Application-Specific Mitigation Plan](#)

[Robokiller](#)

[Know Your Customer](#)

[New Subscribers](#)

[Existing Subscribers](#)

[SwitchUp](#)

[Know Your Customer](#)

[New subscribers](#)

[Existing subscribers](#)

[TapeACall](#)

[Know Your Customer](#)

[New subscribers](#)

[Existing subscribers](#)

[TextKiller](#)

[Know Your Customer](#)

[New subscribers](#)

[Existing subscribers](#)

[TrapCall](#)

[Know Your Customer](#)

[New subscribers](#)

[Existing subscribers](#)

Overview

Bending Spoons Operations S.p.A. (“**Bending Spoons**”) provides the following OTT-based digital products through the following mobile applications which act as voice service providers (each an “**Application**” and, collectively, the “**Applications**”):

- Robokiller
- SwitchUp
- TapeACall: Call Recorder (“**TapeACall**”)
- TextKiller
- TrapCall

More information on each application is provided in dedicated sections in this document. Except as set out in such dedicated sections, the information in this document generally applies to all Applications.

Outbound traffic generated from an Application and its supporting platform is sent through trusted downstream telecommunication service providers (“**DTSP**”). The filings of each DTSP can be found in the Federal Communications Commission (“**FCC**”) [Robocall Mitigation Database](#) (“**RMD**”) and, as of this date, include a “Complete STIR/SHAKEN Implementation”. In particular, Inteliquent, Inc. signs the Application’s outbound traffic with their STIR/SHAKEN certificates. Therefore, Bending Spoons does not have its own STIR/SHAKEN Implementation. Similarly, Bending Spoons does not have an Operating Company Number (OCN).

Moreover, the DTSP have systems in place to notify Bending Spoons if a certificated call made through an Application has been subsequently identified as spam or risk. In response to this, Bending Spoons takes action to remove any Application traffic or user that is identified as originating fraudulent traffic upon receipt of such a notification. This is done by tracing the Direct Inward Dialing (“**DID**”) back to the identified user and eventually suspending or terminating the user’s access to the Application.

Bending Spoons leases DIDs from upstream service providers through the Applications and does not directly own North American Numbering Plan number blocks. Similarly, Bending Spoons does not lease, resell, or otherwise make such numbers available to other service providers. The Applications do not provide origination or termination services to any other service provider.

Bending Spoons operates on the Voice over Internet Protocol (VoIP) network through the Applications. Outbound calls might reach the Public Switched Telephone Network (PSTN) through its DTSP.

The Applications do not support SIP Trunking, SIP Registration, Application Programming Interfaces, or other integrations for mass calling. The Applications are not designed to support automated calling or outgoing pre-recorded messages.

Terms of Service

New users are required to agree to an Application’s Terms of Service. While each Application has its specific set of terms and conditions, the following terms apply to all Applications:

- **Prohibited Uses:** Users are forbidden from using the Applications for any illegal or unauthorized purpose, including for sending or distributing unsolicited or bulk electronic communications and spam. Users must use the Applications in accordance with applicable laws, including regulations related to telecommunication, privacy, and consumer protection laws.
- **Account Termination upon violations:** Any violation of the Terms of Service may result in the suspension or termination of the user’s account and their access to the Application.

Suspicious Activity Investigations

In connection with the Applications, Bending Spoons will use best efforts to provide an initial response within 24 hours to any traceback requests from the FCC, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

Bending Spoons proactively monitors system metrics to detect suspicious traffic within the Applications. When such activity is identified, Bending Spoons follows predefined investigation procedures which typically include, but are not limited to:

- Analyzing recent and past user traffic and account activity records, and benchmarking them against the expected trends;
- Checking that recent system issues or new releases have not introduced erratic behavior that could affect the experienced suspicious activity;
- Examining the entire traffic path, including upstream and downstream SIP packet validity where possible;
- Collaborating with upstream and downstream providers to collect further evidence;
- Contacting the user to verify their use case and validate their association with the suspicious activity; and
- Taking action based on findings, which actions may include enforcing the Terms of Service and terminating violating accounts with notification to account holders.

Public Safety

The Applications accept traffic from domestic and foreign voice service providers, gateway and non-gateway intermediate providers only if that provider's filing appears in the RMD and its filing has not been de-listed pursuant to an enforcement action. Compliance is verified through periodic manual checks of the RMD.

Bending Spoons uses reasonable efforts to safeguard public safety in the development and distribution of the Applications. In this regard, the Applications do not block voice calls to 911. However, it should be noted that, on SwitchUp and TapeACall, users are not supposed to place calls to 911 through the DID associated with the user as they should use their own phone number instead. Therefore, if a SwitchUp or TapeACall user tries to call 911 from the relevant app, an error message is displayed prompting the user to place the call from their own phone number. This ensures no other "association layer" is added to the caller identity ladder and thus fosters safeguarding public safety. Furthermore, Bending Spoons uses reasonable efforts to prevent the blocking of calls from public safety answering points and government emergency numbers.

No Former Formal Actions or Investigations

In the prior two years, Bending Spoons has not been the subject of a formal FCC, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

Plan Updates

This plan and industry best practices will evolve to effectively respond to the dynamic nature of mitigating illegal robocalling. Bending Spoons monitors and will use efforts to monitor industry best practices and continuously improve the internal processes to keep this plan and the systems underlying the Applications up to date in accordance with such practices. In particular, the

Application-Specific Mitigation Plan section is guided by [the NANC Caller Authentication Anchor Trust Working Group's best practices](#) for user vetting.

In the event of any material change to this plan, Bending Spoons will revise its RMD filing within ten days of the update.

Application-Specific Mitigation Plan

Robokiller

Robokiller is a leading OTT spam and unwanted call-blocking application.

Robokiller does not originate new outbound calls. Rather, it can receive calls intended for its users by leveraging call forwarding. This allows Robokiller to analyze incoming call traffic and assign spam risk scores. Based on the user's preferences, it will then take the appropriate action, such as blocking or screening the call. Robokiller's spam protection also extends to voicemail and messages.

To further reduce robocalls, Robokiller offers a lookup webpage where users can check the fraud risk of a specific phone number, report it, or add comments to help the community fight robocalling.

Robokiller actively monitors aggregate metrics to detect large-scale anomalies and prevent widespread fraudulent activity.

While Robokiller uses caller ID-based blocking, call spoofing has made this less effective. To oppose call spoofing, Robokiller deploys the following tools:

- **Audio fingerprinting:** The Application's audio-fingerprinting technology creates a record of a robocaller's unique audio recording and matches it in real-time against a global database of over 1.5 billion phone numbers and millions of audio fingerprints. This allows Robokiller to determine whether it's spam, even if spammers spoof their phone numbers.
- **Call Screening:** Unknown callers are asked to state their name and reason for calling, enabling users to decide whether to answer in real-time.
- **Spam Patrol:** Users can participate in Spam Patrol by reporting spam calls, training the Robokiller algorithm to protect themselves and others from future spam calls.
- **Custom lists:** Users can create personal lists to control who can reach them, blocking or allowing specific callers.

Additionally, if selected by the subscriber, Robokiller can utilize answer bots to respond to spam or fraudulent calls, and consume the spammer's time, acting as a deterrent.

Know Your Customer

New Subscribers

New subscribers are required to provide their telephone number to activate the service and are instructed on how to set up call forwarding and voicemail. The phone number is verified through either an SMS or a call. Additionally, external providers are engaged to validate the number and retrieve the

associated carrier information. Subscribers also receive practice calls to ensure the setup is functioning correctly.

Separate fraud controls are managed by payment processors (such as Apple or Google).

Existing Subscribers

To prevent unexpected traffic, rate limits are enforced at several points in the system, and monitoring and alerting are set up for aggregated metrics.

Through call-forwarding, inbound calls to subscribers are directed to one of the DIDs leased from voice service providers. The system tracks a subscriber's association with a DID, but its dynamic nature does not impact the effectiveness of the analysis or the spam risk the user is exposed to, and it's driven by resource optimization within our systems.

SwitchUp

SwitchUp is a virtualized “second phone line” mobile application that both originates and receives calls.

For outbound calls, the subscriber's phone number contacts a DID (leased from service providers) associated with our system. The system then connects the subscriber's SwitchUp DID to the destination number via one of the service providers, which signs the call on the subscriber's behalf.

For inbound calls, the call is first received by the subscriber's SwitchUp DID and then forwarded to their phone number. Regardless of the subscription tier, SwitchUp offers spam protection using the same proprietary technologies as other Applications. When a legitimate call is received, the caller's number and the SwitchUp logo are displayed, helping the subscriber decide whether to answer. If a call is marked as spam, it is automatically terminated and shown as blocked in the Application's interface.

Subscribers can also set *Do Not Disturb* schedules on their virtualized numbers, preventing calls (including spam) from reaching them during specific times, such as outside business hours.

Know Your Customer

New subscribers

New subscribers must log in through Google or Apple authentication. Once authenticated, they're assigned a DID (leased from our providers) with a verified reputation.

Separate fraud controls are managed by payment processors (such as Apple or Google).

Existing subscribers

There are rate limits on login attempts to prevent abuse.

Outgoing traffic is also rate-limited, with breaches leading to account suspension and, in cases of mass spamming or other violations of the Terms of Service, termination of the fraudulent account. Monitoring and alerting are in place to track aggregated metrics. Even with top-tier subscription plans, subscribers

are limited to a maximum of three virtualized numbers, alongside strict rate limits, to prevent the generation of mass traffic.

When making outgoing calls through SwitchUp, the subscriber's identity cannot be anonymized, and this setting cannot be modified.

TapeACall

TapeACall is a mobile call-recording application used primarily for recording inbound and outbound calls.

To record an outbound call, the app dials a specific DID leased from providers. The system forwards the call to the intended recipient, recording it and signing it as required by the service provider.

Know Your Customer

New subscribers

New subscribers must verify their phone number via Google Firebase, or SMS/call if Google Firebase is unavailable.

Separate fraud controls are managed by payment processors (such as Apple or Google).

Existing subscribers

While TapeACall does not offer spam protection services, as this is beyond the Application's functionality, it has monitoring and alerting systems in place to prevent existing subscribers from recording a disproportionate number of calls.

TextKiller

TextKiller is a mobile application designed to automatically block spam text messages in near real-time using techniques such as fingerprinting.

Users can customize their experience by setting up block-lists and allow-lists for specific numbers and keywords, filtering spam messages from legitimate ones.

Additionally, TextKiller offers functionality to filter all messages from senders outside of the subscriber's contact list, providing an additional layer of security against unsolicited texts.

Know Your Customer

New subscribers

New users are required to register through telephone number, upon its verification.

Separate fraud controls are managed by payment processors (such as Apple or Google).

Existing subscribers

Rate limits are in place at several points of the system to prevent unexpected traffic. Similarly, monitoring and alerting are in place for several aggregated metrics.

TrapCall

TrapCall is a mobile application designed to unmask and block unwanted calls, providing users with enhanced control over their incoming communications.

TrapCall reveals the phone numbers behind blocked, private, restricted, and “No Caller ID” calls, allowing users to identify anonymous callers. TrapCall also automatically blocks spam, telemarketing, and robocalls using a continuously updated global spam list, preventing these calls from reaching the user. Additionally, users can create personal block lists to prevent specific numbers from contacting them. When a blocked number attempts to call, the caller hears a message stating the user’s number is disconnected, discouraging further attempts.

TrapCall does not generate new outbound calls. Rather, it receives calls intended for our users by leveraging call forwarding. The Application’s systems can analyze the traffic and possibly unmask the caller, leveraging third-party databases in this manner. Then, it reaches the user, revealing the caller's identity. When the caller is unknown, they are prompted to state their name before the call is forwarded to the user.

Know Your Customer

New subscribers

New subscribers must provide a telephone number, which is verified before proceeding further with the onboarding process.

Separate fraud controls are managed by payment processors (such as Apple or Google).

Existing subscribers

Rate limits are implemented throughout the system to prevent unexpected traffic. Similarly, monitoring and alerting measures are in place to track key aggregated metrics for system reliability.

Inbound calls to subscribers are routed through DIDs leased from voice service providers, with the system dynamically associating each subscriber to a DID. This dynamic assignment optimizes resources without affecting call analysis or increasing spam risk.