



Robocall Mitigation Plan

v2.3



Table of Contents

1. General Information	3
a. Certification of Compliance with FCC Requirements	3
2. Robocall Mitigation Program	4
3. Customer Vetting (“Know Your Customer”)	5
a. Role in the Call Chain	5
b. User Registration	5
c. User Metadata	5
d. Number Allocation	5
e. Terms of Service Enforcement	5
4. Detailed Robocall Mitigation Measures	6
a. Service Architecture	6
b. Trusted Upstream Provider Partnership (“Know Your Upstream Provider”)	6
c. Advanced Technology Deployment	6
d. Real-Time Monitoring	7
e. Partnership with Cloudmark	7
f. Comprehensive Investigation Protocol	7
g. Traffic Pattern Analysis	7
5. Call Blocking for Users	7
6. Call Blocking for non-RMD members	8
7. Traceback / Enforcement Cooperation	8
8. Principals, Affiliates, Subsidiaries, and Parent Companies	8
9. Contact Information	9



1. General Information

a. Certification of Compliance with FCC Requirements

In alignment with the Federal Communications Commission's (FCC) regulations and directives, this document outlines the Robocall Mitigation Program (RMP) of **textPlus, Inc.** ("**textPlus**"), designed to thwart unlawful robocalls on our network as a Voice Service Provider. Definitions herein adhere to those established under 47 C.F.R § 64.6300 unless specified otherwise.

Company Overview

textPlus offers innovative voice and messaging communications targeting consumers for peer-to-peer and group communications via app. **textPlus** has fully embraced digital technology to ensure the highest quality of service, operating on a modern infrastructure that supports our commitment to user safety and satisfaction.

As a Voice Service Provider, **textPlus** does not act as an Intermediate Provider. We directly connect with Sinch, our sole Intermediate Provider in the United States, ensuring that all voice traffic originated or terminated by **textPlus** is efficiently managed. Our Operating Company Number (OCN) is 128K, reflecting our registered status and operational scope.

Filing of RMP and Implementation of STIR/SHAKEN

textPlus has diligently submitted this RMP to the FCC, certifying that:

- This RMP governs all calls originating on our network.
- Our previous certification remains unrevoked by the FCC.
- We have not been barred from submitting to the Robocall Mitigation Database (RMD) by the FCC.

In compliance with 47 C.F.R. § 64.6305, **textPlus** proudly certifies the full implementation of STIR/SHAKEN protocols across our network. This ensures that every call we originate



aligns with the standards set forth in 47 C.F.R. §§ 64.6301, reinforcing our dedication to combating robocall abuse.

Our RMP, accessible within the RMD, lays out the "reasonable steps to avoid originating illegal robocall traffic." It underscores our pledge to respond within 24 hours to traceback requests from the FCC, law enforcement, and the industry's traceback consortium. Our cooperation extends to aiding investigations to halt any illicit robocall activities utilizing our services.

As mandated by 47 C.F.R. § 64.6305, textPlus's role in the call chain is defined as:

- A Voice Service Provider obligated to implement STIR/SHAKEN, serving end-users directly.

In accordance with FCC Rule 64.6305, textPlus attests that over the past two years, neither textPlus nor any related entity under common ownership has been implicated in any formal actions or investigations by the FCC or other regulatory bodies for facilitating or being complicit in illegal robocalls or spoofing activities.

2. Robocall Mitigation Program

textPlus is committed to stopping illegal robocalls from originating and terminating on our network, which is expressly against the textPlus Terms of Service. This Robocall Mitigation Plan describes the specific measures that we have implemented to detect and prevent this illegal activity from happening on our network. These processes and capabilities are reviewed frequently for effectiveness and are often expanded and improved based on learnings and industry best practices. Through rigorous adherence to FCC guidelines, innovative technological safeguards, and a proactive approach to robocall mitigation, we are dedicated to ensuring our users enjoy a safe and seamless communication experience.



3. Customer Vetting (“Know Your Customer”)

a. Role in the Call Chain

As a voice service provider, textPlus exclusively serves end-users for peer-to-peer communication, with no business use allowed. Our service model and Terms of Service are crafted to deter misuse by robocallers.

b. User Registration

Users need to register to become a textPlus subscriber via either iOS or Android apps. All users need to register using “Sign in With Apple” or “Google Sign-in” to become a textPlus user, adding an additional layer of security built-in to those platforms.

c. User Metadata

Upon registration, we collect basic metadata as available from the user which can include email, network information, device information, reported geo-location, etc. to use for law enforcement and/or traceback requests.

d. Number Allocation

Our subscribers can request a TN (“telephone number”) that is assigned by the platform to their internal UUID, subscribers have no way to spoof the TN as the platform will automatically set the Caller-ID based on this UUID when outbound calls to PSTN are placed.

e. Terms of Service Enforcement

Our subscribers are bound by the textPlus Terms of Service, which encompass provisions specifically designed to combat robocalling and ensure the integrity of our communication services. These provisions include (a) strict prohibitions against the use of textPlus services for any form of malicious activities, including robocalling and spamming, (b) the express authority for textPlus to terminate services to any subscriber at our discretion, with or without prior notice, particularly in cases of suspected abuse or violations of our Terms of Service, and (c) the unequivocal right of textPlus to access



subscriber accounts and records as part of our efforts to investigate any complaints, allegations of misuse, or unauthorized uses of our services, with such investigations conducted confidentially unless disclosure is mandated by legal requirements. Additionally, textPlus retains the prerogative to update or modify its Terms of Service at any given time without prior notification, placing the onus on our subscribers to remain abreast of and comply with the current Terms of Service, thereby upholding our commitment to mitigate robocalling and maintain service integrity.

4. Detailed Robocall Mitigation Measures

a. Service Architecture

The textPlus platform restricts accounts to making one call at a time per account, significantly reducing the attractiveness of our service to robocallers who rely on the ability to make concurrent calls at scale.

b. Trusted Upstream Provider Partnership (“Know Your Upstream Provider”)

textPlus has maintained a decade-long partnership with our upstream voice provider, Sinch. This relationship has fostered meaningful familiarity, trust, and has been instrumental in enhancing our security capabilities. textPlus leverages Sinch’s advanced security services, including a variety of network tools, such as call randomizers, ANI management, proactive blocking based on Do-Not-Originate lists, and whitelisting of known legitimate numbers, we also receive immediate alerts on unusual usage patterns, enabling us to promptly investigate and address potential threats.

c. Advanced Technology Deployment

All our apps employ IP detection and state-of-the-art device fingerprinting technologies to verify the authenticity of devices and the quality of IP addresses accessing our service. This approach is crucial in thwarting attempts by scripted attacks from untrusted networks. (Anonymous IPs, VPNs, Proxies, Data Centers, Clouds, etc. are frequently blocked from accessing our services).



d. Real-Time Monitoring

textPlus actively monitors for spam and robocalling activity indicators, including a high volume of short-duration calls, an imbalance between outgoing and incoming calls, the number of unique destinations dialed, and call velocity. These metrics enable us to detect and respond to potential abuse in real-time.

e. Partnership with Cloudmark

Our collaboration with Cloudmark, a leader in carrier-grade messaging security, extends our capability to detect and mitigate threats. Through this partnership, we have also identified and neutralized voice-related threats, underscoring our proactive stance against robocalling and spam.

f. Comprehensive Investigation Protocol

We investigate all reports of spam, abuse, or robocalling received through any of our communication channels. This thorough approach ensures that we rapidly address and mitigate any identified issues.

g. Traffic Pattern Analysis

Our system is configured to alert us to any deviations from normal traffic patterns, including changes in call volume, duration, and the ratio of inbound to outbound calls. This enables us to swiftly respond to anomalies that could indicate robocalling activity. We do not utilize third-party vendors for traffic analytics.

5. Call Blocking for Users

textPlus has built-in functionality in its mobile applications to offer any user the possibility to block incoming calls from unwanted sources. textPlus also responds to recipient requests to investigate unwanted traffic to any TN in the world.



6. Call Blocking for non-RMD members

textPlus doesn't provide commercial or reseller services and all our traffic is routed through a small number of registered members of the RMD that are major US telecom providers and will block inappropriate upstream traffic as well as traffic from non-RMD members for us.

7. Traceback / Enforcement Cooperation

textPlus is fully committed to cooperating with industry-wide traceback efforts to identify and mitigate the sources of illegal robocalls. Upon receiving traceback requests from recognized industry groups or regulatory bodies, we will:

- **Prompt Response:** Ensure our dedicated team responds to traceback requests within 24 hours, providing relevant information to aid the investigation.
- **Investigation Support:** Utilize our advanced analytics capabilities to trace the call's origin within our network, offering insights and data to assist in pinpointing the source of illegal activity.
- **Remedial Actions:** In cases where illegal activity is confirmed, textPlus will take immediate steps, such as blocking the offending traffic and suspending or terminating the responsible customer accounts, in accordance with our Terms of Service.

8. Principals, Affiliates, Subsidiaries, and Parent Companies

Principals

textPlus, Inc. is managed and controlled by the following executives and investors:

- **Scott Lahman**, CEO and Board Member

Investors:

- **Jason Schretter**, Board Member, representing Raine Partners
- **Hamet Watt**, Board Member, representing Upfront Ventures, a venture capital firm



- **Samer Bishay**, Board Member and CEO of Iristel, a telecommunications firm based in Canada

Affiliates and Parent Companies

textPlus, Inc. has no parent companies or affiliates.

Subsidiaries

textPlus, Inc. has one inactive subsidiary:

textPlus Labs, Inc.

This subsidiary has been inactive since 2015 with no activity whatsoever.

9. Contact Information

Points of contact to handle traceback requests:

- Level 1: Calling Fraud Response Team: callfraud@textplus.com // +1 310 910 1461
- Level 2: Joel Serrano: joel@textplus.com // +1 310 896 8516
- Level 3: Alex Scissors: alex@textplus.com // +1 510 584 9801



Document Changelog

Consistent with FCC regulations, **textPlus** will submit updates to this filing with any updates, changes and improvements within 10 business days of those changes being made.

The following chart is used to log all version submissions of this document:

Version	Date Submitted	Author	Description	Pages affected
1.0	2021-09-22	Joel Serrano	Initial	All
2.0	2024-02-26	Joel Serrano	Update RMP	All
2.1	2024-10-17	Scott Lahman	Added Section 8 regarding our principals, affiliates, subsidiaries and parent companies	Pages 8-9
2.2	2026-01-23	Scott Lahman	Added additional details to section 4(g)	Page 7
2.3	2026-02-23	Joel Serrano	Updated Index Replaced “Inteliquent” with “Sinch” in Sections 1(a) and 4(b) to reflect current carrier naming. Revised Section 4(d) to include additional monitoring metrics (unique destinations dialed and call velocity).	Page 2 Pages 3, 6 Page 7