Zipwhip Messaging Policies and Best Practices

Version 1.1, January 2019

Version History

Version	Version Date	Authors	Notes
Version 1.0	March 1, 2017	Anna Henningsgaard James Lapic Anthony Riemma	First release
Version 1.1	January 1, 2019	Brad Biltz James Lapic Carter Harris	New Sections: 3.1.1 3.3.6 3.3.7 4.1.6 4.1.7 4.1.8 4.2.4. 4.2.5 Updated Branding

Zipwhip, Inc.

1501 1st Avenue South
Seattle, WA 98134
Phone: 1-855-ZIPWHIP (1-855-947-9447)
Email: noc@zipwhip.com

Contents

1.0 Introduction

The Zipwhip text messaging network supports more traffic throughput than traditional person-to-person text messaging channels. Our network is designed to facilitate high-quality, high-integrity A2P business communications, not spam or unconsented messaging. To protect both networks and consumers from abuse, Zipwhip enforces a basic code of conduct, which provides best practices for sending messages and content generation. All users of the Zipwhip network, including users of software, API, or gateway services, are held to the same standards and expectations.

1.1 Scope and Objectives

In designing these policies and best practices, Zipwhip strives to:

- Design minimal, common sense policies;
- Empower consumer choice;
- Support transparency and open communication with businesses; and
- Stay flexible, so that rules can adapt and evolve.

Although these best practices do not offer legal advice or guidance, the messages sent through the Zipwhip network should be consistent with relevant laws and regulations, including (but not limited to) the FCC Telephone Consumer Protection Act (TCPA).

1.2 Enforcement

Zipwhip may, at its discretion, review accounts for compliance with these policies and best practices. Non-compliance could result in the suspension of sending rights for a provisioned phone number; restriction of high-throughput access; suspension of provisioning rights for new phone numbers; and/or suspension of all network services.

Repeated non-compliance with these policies may result in termination of all network services.

1.3 Revision and Adoption

This guide is updated as needed, and stakeholders are typically notified 30 days in advance.

2.0 Code of Conduct

Wireless network operators (Operators) support commercial, non-consumer traffic to varying degrees. All Operators take measures to protect both their networks and consumers from spam. Zipwhip is contractually obligated to support basic safeguards for high-throughput commercial traffic.

2.1 Requirements

The Code of Conduct contains five straightforward requirements for message senders:

2.1.1 Only valid companies in good standing may engage in high-throughput traffic

To protect the integrity of text messaging networks and services, including the business operations of legitimate service providers, message senders of high-throughput text messaging must pass a basic validation during onboarding with the service provider and maintain good standing.

2.1.2 The consumer must give appropriate consent for the given message type

For more information about consent parameters, see Section 3.1.

2.1.3 Consumer opt-in and opt-out must work correctly

Consumer opt-in and opt-out functionality is enforced at the network level via the STOP and UNSTOP keywords. This functionality cannot be disabled for service providers or message senders. Message senders have additional obligations for processing of opt-out messages that must be honored. For more information about opt-in and opt-out, see section 3.2.5.

2.1.4 Phishing, spam, illegal and unwanted illicit content is prohibited

Message content that deceives or threatens consumers, including phishing, is not permitted. Even if a consumer consents to receive messages, the messages must not be deceptive; TCPA compliance alone does not satisfy this condition. For more information about prohibited content, see section 4.2.

2.1.5 Creative methods to evade these requirements is prohibited

The spirit of these requirements is straightforward; to protect both consumers and networks. Message senders acting in bad faith to thwart or undermine the spirit of these requirements are addressed on a case-by-case basis.

3.0 Best Practices for Sending Messages

3.1 Consent (Opt-In)

The message sender must obtain proper consumer consent for each message sent. The type of consent that is required depends on the type of message content sent to the consumer. The table below includes the types of messaging content and the associated consent that is required. Consumers can revoke consent at any time and in any way. Consumer opt-out requests must be honored, whether they are made by phone call, email, or text.

Types of Messaging Content & Required Consent		
Conversational	**Informational**	**Promotional**
Conversational messaging is a back-and-forth conversation that takes place via text. If the consumer texts into the business first and the business responds quickly with a single message, then it's likely conversational. If the consumer initiates the conversation and the business simply responds, then no additional permission is required.	Informational messaging is when a consumer gives their phone number to a business and asks to be contacted in the future. Appointment reminders, welcome texts, and alerts fall into this category because the first text sent by the business fulfills the consumer's request. A consumer should agree to receive texts when they give the business their mobile number.	Promotional messaging is a message sent that contains a sales or marketing promotion. Adding a call-to-action (such as a coupon code to an informational text) may place the message in the promotional category. Before a business sends promotional messages, the consumer must agree in writing to receive promotional texts. Businesses that already ask consumers to sign forms or submit contact information can add a field to capture the consumer's consent.
First message is always sent by the consumer Two-way conversation Message responds to a specific request	First message is sent by the consumer or business One-way alert or two-way conversation Message contains information	First message is sent by the business One-way alert Message promotes a brand or product Prompts consumer to buy something, go somewhere, or otherwise take action
IMPLIED CONSENT If the consumer initiates the text message exchange and the business only responds to each consumer with relevant information, then no verbal or written permission is required.	EXPRESS CONSENT The consumer should give permission before a business sends them a text message. Consumers can give permission over text, on a form or website, or verbally. Written permission also works.	EXPRESS WRITTEN CONSENT The consumer should give written permission before a business sends them a text message. Consumers can sign a form, or check a box, to allow promotional text messages. Participation in text promotions should never be a requirement.

Consent is only to be obtained from the individual consumer and not on behalf of another individual. Opt-in data and consent may never not be shared, sold or bought.

3.1.1 Double Opt-In

Zipwhip does recommend obtaining a secondary “Double Opt-In" in cases where the consent was initially collected out of band, (i.e. phone call, web form, etc.). Double Opt-In is the practice of confirming an opt-in via text by requesting for the consumer to reply “Yes” to confirm in participating in text messaging with the business. This gives the business a confidence in receiving proper subscriber consent and protecting against incorrect mobile number collection during an out of band opt-in.

Examples of Double Opt-In:

- “Reply Yes to confirm that you want to receive text messages from {Business Name}, Reply STOP to unsubscribe”
- “{Brand Name}: Reply YES to confirm receiving SMS/MMS messages {link to Terms of Service} Reply “STOP” to unsubscribe”

3.2 Revoking Consent (Opt-Out)

Zipwhip supports mandatory opt-out compliance by supporting the STOP keyword at the network level. This opt-out system is active by default across all accounts on the Zipwhip network.

A STOP request blocks all text message exchanges between an individual mobile number and a text-enabled business number. A consumer can opt back in at any time by replying with the keyword UNSTOP.

3.2.1 Consumer notification

Zipwhip recommends the best practice of notifying the consumer of their ability to opt-out from future messages from the message sender. This is especially important when sending informational or promotional messages. An example would be to include the sentence, “Reply STOP to unsubscribe” to the end of the message sent to the consumer. We recommend sending this communication on the first message and at least every 5th message or at least once a month for continued consumer awareness, if not on every message.

3.2.2 Opt-Out keywords and message

A consumer can opt out of communication with any message sender on the Zipwhip network by texting the keyword “STOP” to the message sender’s phone number. The keyword is not case sensitive and triggers an opt-out only when sent as a single word with no punctuation or leading spaces (any trailing spaces are trimmed). If the consumer uses the opt-out keyword within a sentence, then an opt-out is not triggered.

Examples of valid opt-out messages:

- “STOP”
- “Stop”
- “stop”
- “STop”

Examples of invalid opt-out messages:

- “Hey can you stop texting me?”

- “Stop it!”
- The opt-out confirmation message returned to a consumer is generic and gives instructions on how to opt back into service again with the message sender’s phone number.

Opt-out confirmation message:

> *NETWORK MSG: You replied with the word "STOP" which blocks all texts sent from this number. Text back "UNSTOP" to receive messages again.*

3.2.3 Opt-In keywords and message

A consumer can opt back in at any time to receive messages by texting the keyword “UNSTOP” to a message sender’s phone number. The keyword is not case sensitive and triggers an opt-in only when sent as a single word, with no punctuation or leading spaces (any trailing spaces are trimmed). If the consumer uses the opt-in keyword within a sentence an opt-in is not triggered.

Examples of valid opt-ins:

- “UNSTOP”
- “Unstop”
- “unstop”
- “UNStop”

Examples of invalid opt-ins:

- “Hey can you enable me again?”
- “Unstop me!”

The message returned to a consumer is generic and informs the consumer they can start two-way texting with the message sender’s phone number again.

Opt back in confirmation message:

> *NETWORK MSG: You have replied "unstop" and will begin receiving messages again from this number.*

3.2.4 Notification of Opt-Out/Opt-In

Depending on the connectivity with the Zipwhip network, opt-out and opt-in messages trigger either an SMPP message or HTTP web hook event to the message sender. This is the default behavior unless otherwise specified during the onboarding process.

3.2.5 Expectation upon receipt of Opt-Out/Opt-In

A message sender must act upon every opt-out event sent to them from Zipwhip. The opted-out consumer phone number must be removed from all distribution lists and be logged as “opted out” from all text messaging communications with the business. This ensures that future messages are not attempted, and consumer consent is honored.

3.2.6 Sending to a consumer that has opted out

If a message sender attempts to send a text message to a consumer that has opted out of communications with the specific phone number of the sender, then an error message is returned. The error message is returned within

a final delivery receipt and has a status code of 1110 (decimal)/456 (hex). If final delivery receipts are not enabled, then no notification is presented to the message sender. Delivery of final delivery receipts is the default behavior unless otherwise specified during the onboarding process.

3.3 Disallowed Sending Practices

If a message sender is observed performing any of the disallowed sending practices that are listed below, then an account review is performed. The review can result in the suspension of sending rights for a provisioned phone number; restriction of high-throughput access; suspension of provisioning rights for new phone numbers; and/or suspension of all network services.

Message senders are expected to enforce restrictions on their own networks to prevent these sending practices at the intake source.

3.3.1 Continued sending to opted out consumers

When a consumer opts out, they should no longer receive messages from that message sender. If they do receive messages, then it's likely that the opt-out event was either not processed or processed incorrectly within the message sender's network. Continued sending to opted-out consumer could result in the message sender to be audited or suspended.

3.3.2 Opt-Out avoidance

Message senders should use the word "STOP" to identify proper opt-out as outlined in 3.2.2 and using other keywords in attempt to avoid opt-out is prohibited. Continued attempts to evade the Stop keyword could result in the message sender to be audited or suspended.

Examples of disallowed opt-out:

- "Reply 3 to no longer receive messages"
- "Reply NO to stop"

3.3.3 High opt-out rate

Message senders receiving high volumes of opt-outs could be an indication of poor sending practices or that the opt-in data may be in question. When the daily opt-out rate on a sending phone number is 5% or greater, then the account is flagged for monitoring which may result in immediate suspension of services.

The daily opt-out rate on a phone number is defined as the total number of unique consumer phone numbers that received a successful message divided by the unique opted out consumers that were sent messages within a 24-hour period.

3.3.4 Snowshoe sending

Snowshoe sending is defined as a technique used to spread messages across many source phone numbers, specifically to dilute reputation metrics and evade filters. Zipwhip actively monitors for snowshoe sending. If we discover snowshoeing, then the sending phone numbers may have their sending rights immediately suspended.

3.3.5 URL cycling

When message senders use URLs but cycle the domain or subdomain for every message they send for the specific purpose of diluting reputation metrics and evading spam filters. This sending practice may result in immediate suspension of services.

3.3.6 URL redirects/forwarding

When message senders include a URL in the message and the URL will redirect to another URL and then redirect again and so on. This practice can go multiple layers deep resulting in the consumer not knowing what website they will eventually be taken to. This sending practice may result in immediate suspension of services.

3.3.7 Number cycling

Number cycling is when a message sender uses a number until it begins to show signs of deliverability degradation and then the sender discards the number for a new one and repeats the process. This sending practice results in ruining the reputation of the numbers and may result in immediate suspension of services.

4.0 Best Practices for Message Content

Zipwhip recommends the following best practices when generating content and choosing source phone numbers. High quality, well-formatted content is more likely to be opened and read by a consumer and less likely to be mistaken as spam by consumers, Operators, and Zipwhip.

Zipwhip does not pre-approve or whitelist messaging content or phone numbers. We may review any message content as part of an account review.

4.1 Recommendations for Content Creation

These best practices make messages more valuable to consumers and less likely to trigger real-time content analysis from flagging messages incorrectly as spam.

4.1.1 Use one recognizable number

Each business or program should use one primary phone number. Using a single number for both text and voice calls is recommended. The business can run all of their business traffic on one phone number.

4.1.2 Use one recognizable domain name

Each program should be associated with a single business's web domain. Although a full domain is preferred, a branded short URL may be used to deliver custom links. This adds continuity with the consumer to improve brand awareness as well as increases confidence in the link.

4.1.3 Use natural language

You should use natural language in your messages, which means that you do not use non-standard spellings. For example, "H! h0w ar3__you do1ng?" is a nonstandard spelling.

4.1.4 Direct consent

You should collect the consumer consent yourself, and not use consent acquired from a third party. The consumer is expecting a relationship with the business they interacted with. Please reference 3.1 for further information on consent.

4.1.5 Set expectations on frequency

You should set the proper expectation with the consumer on how many messages they can expect to receive. If you are sending 5 texts a month, then disclosing "5/msg a month" on the first interaction will result in a positive consumer experience.

4.1.6 Business recognition

You should include the business name within the message to ensure that the consumer knows who they are interreacting and not attempt to hide the identity.

4.1.7 Length of message

SMS stands for “Short Message Service” and this should be taken into consideration when formatting a text message. Even though concatenated message exist we recommend not sending more than a 250-character message to keep the medium a short message platform.

4.1.8 Ending with “Stop”

To ensure that the consumer feels that they have control to remove themselves from text message communication, you should end your messages with the Opt-out keyword “Stop” as defined in 3.2.2.

4.2 Inappropriate Content

If a message sender is observed sending any of the below listed disallowed content, then an account review is performed. This review can result in the suspension of sending rights for a provisioned phone number; restriction of high-throughput access; suspension of provisioning rights for new phone numbers; and/or suspension of all network services.

Message senders are expected to enforce restrictions on their own networks to prevent these types of content at the intake source. These categories can change quickly depending on the current market trends. For the most recent list of inappropriate content please send in a request to either reportfraud@zipwhip.com or noc@zipwhip.com

4.2.1 Phishing

Phishing is the practice of sending messages that appear to come from reputable companies but in fact trick consumers into revealing personal information, such as passwords and credit card numbers.

4.2.2 Fraud or scam

Any messages that constitute a fraud or scam, which involves wrongful or criminal deception intended to result in financial or personal gain, are prohibited. These messages generally involve money and/or some sort of business transaction.

4.2.3 Deceptive Marketing

Marketing messages must be truthful, not misleading, and, when appropriate, backed by scientific evidence in order to meet the standard held by the Federal Trade Commission’s (FTC) Truth In Advertising rules. The FTC prohibits unfair or deceptive advertising in any medium, including text messages.

4.2.4 High-Risk Financial Services

Financial services that are considered high risk to the end consumer are prohibited due to the deceptive or unfair nature of these services. These messages generally involve loans, credit repair or debt forgiveness.

4.2.5 Illegal Substances or Activities

Messages that include information about substances or activates that are explicitly against Federal or State statutes are prohibited.

5.0 Monitoring

Zipwhip works with industry leading spam containment vendors and monitors consumer complaints. These practices promote a sustainable model for healthy commercial texting, which is good for both consumers and message senders.

5.1 Monitoring

Zipwhip utilizes different methods to gather feedback on adherence to the code of conduct and best practices. Some common methods are listed below.

5.1.1 Consumer complaints

Major operators in North America support consumer driven spam controls. Their mobile subscribers can forward unwanted or unconsented text messages to a dedicated short code, 7726 (it spells “SPAM” on a standard keypad).

Zipwhip monitors consumer complaints sent to this service for numbers on our network. If multiple complaints are received for a sender, then a notification is sent to the message sender that includes the source phone number, destination phone number, timestamp, and original Zipwhip message ID that was given to the message sender upon message submission. Upon receipt, the service provider must provide proof of TCPA compliant opt-in for those specific messages. They must also provide an overview of the messaging campaign and its opt-in process that the unwanted message was a part of.

If a large amount of unwanted or unconsented messages are reported on a source phone number, then that number may have sending rights immediately suspended while opt-in is being confirmed.

5.1.2 Opt-out rate

Zipwhip tracks the opt-out rate on every source phone number that is active on the Zipwhip network. When the daily opt-out rate on a sending phone number is 5% or greater, then the account is flagged for monitoring which may result in immediate suspension of services.
The daily opt-out rate on a phone number is defined as the total number of unique consumer phone numbers that received a successful message divided by the unique opted out consumers that were sent messages within a 24-hour period.

5.1.3 Real-time content analysis

Zipwhip works with industry leading risk mitigation containment vendors to analyze message content. Real-time analysis is used to identify if a message falls outside of the code of conduct or best practices. The results of these analysis can result in suspension or termination of message sending privileges on specific traffic and or the entire account.

6.0 Resources

This section includes links to industry resources that may be helpful as a message sender starts to craft messaging content.

CTIA Messaging Interoperability Guidelines
https://api.ctia.org/docs/default-source/default-document-library/170119-ctia-messaging-principles-and-best-practices.pdf

MMA Best Practices
http://www.mmaglobal.com/taxonomy/term/2820

M3AAWG Best Practices
https://www.m3aawg.org/sites/default/files/M3AAWG-Mobile-Messaging-Best-Practices-Service-Providers-2015-08.pdf

Telephone Consumer Protection Act (TCPA) Omnibus Declaratory Ruling (FCC 15-72)
https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-72A1.pdf

FTC Truth in Advertising
https://www.ftc.gov/news-events/media-resources/truth-advertising

Zipwhip Terms of Service

https://zipwhip.com/terms

Zipwhip Acceptable Use Policy

https://www.zipwhip.com/terms/#acceptable-use-policy

Zipwhip, Inc.

1501 1st Avenue South
Seattle, WA 98134
Phone: 1-855-ZIPWHIP (1-855-947-9447)
Email: noc@zipwhip.com