MESSAGING REQUIREMENTS AND CODE OF CONDUCT

The Code of Conduct contains straightforward requirements for message senders.

1. Only 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. The consumer must give appropriate consent for the given message type.

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.

4. Phishing, spam, and unwanted illicit content is prohibited.

5. 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.

Creative methods to evade these requirements are 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.

BEST PRACTICES FOR SENDING MESSAGES

Consumers should always be given the choice to receive or block text messages from a specific message sender. This principle underpins the requirements for the opt-in and opt-out mechanisms. In addition, the Federal Communications Commission (FCC) enforces rules under the Telephone Consumer Protection Act (TCPA) to protect consumers from unwanted calls or text messages. Businesses that send text messages to consumers should be aware of these rules. Violating the TCPA is a serious matter, with statutory damages of $500 to $1,500 per violation (text message sent).

Consent

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 and Required Consent

1. Conversational. 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.

1.1 Characteristics: the first message is always sent by the consumer, two-way conversation, message responds to a specific request

1.2 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.

2. Informational. 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.

2.1 Characteristics: the first message is sent by the consumer or business, one-way alert or two-way conversation, message contains information

2.2 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.

3. Promotional. Promotional messaging is when a message is 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.

3.1 Characteristics: the first message is sent by the business, one-way alert, message promotes a brand or product, prompts consumer to buy something or go somewhere

3.2 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.

Revoking Consent (opt-out)

Carriers require opt-out compliance by supporting the STOP keyword at the network level. This opt-out system is active by default across all accounts. 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.

Consumer Notification

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 initial message sent to the consumer. We recommend sending this communication on at least every 5th informational or promotional message for continued consumer awareness.

Opt-Out Keywords and Messages

A consumer can opt out of communication with any message sender on the 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.

Opt-In Keywords and Messages

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-In Messages

“UNSTOP”
“Unstop”
“unstop”
“UNStop”

Examples of Invalid Opt-In Messages

“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-In Confirmation Message

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

Expectation Upon Receipt of Opt-Out/Opt-In

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

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.

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

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.

2. Opt-out avoidance. If a consumer opts out of communications with a business, then disregarding the consumers opt-out and sending a message from a new phone number from the same business is not allowed.

3. High opt-out rate. The daily opt-out rate on a phone number is defined as the total number of unique consumer phone numbers divided by the unique opted out consumers that were sent messages within a 24-hour period. If the daily opt-out rate on a sending phone number is 5% or greater, then the number is flagged for monitoring. An opt-out rate of 10% or greater on a sending phone number may result in immediate suspension of services.

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. Carriers actively monitor for snowshoe sending. If they discover snowshoeing, then the sending phone numbers may have their sending rights immediately suspended.

5. URL cycling. This practice is defined as the utilization of multiple destination URLs on the same message content for the specific purpose of diluting reputation metrics and evading filters. URL cycling does not include the use of unique “personal” links to give a consumer custom content via a URL shortener or other means.

BEST PRACTICES FOR MESSAGE CONTENT

SignalWire 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 Carriers.

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.

1. Use one recognizable number. Each campaign should use one primary phone number. Using a single number for both text and voice calls is recommended.

2. Use one recognizable domain name. Each campaign should be associated with a single web domain. Although a full domain is preferred, a URL shortener may be used to deliver custom links.

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. 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.

5. Set expectations on frequency. You should set the proper expectation with the consumer for informational or promotional messages. If you are sending 5 texts a month, then disclosing “5/msg a month” on the first interaction is a positive user experience.

Age, Geographic, and Other Restrictions

Additional restrictions may apply if your messaging is related in any way related to alcohol, firearms, gambling, tobacco, or other adult content. You must:

1. Obtain and keep records of consent from every message recipient
2. Ensure that no message recipient is younger than the legal age of consent based on the best geographical knowledge of where the recipient is located.
3. Ensure that the message content complies with the SignalWire Message Requirements and Code of Conduct and all applicable laws of the 4. jurisdiction in which the message recipient is located.
5. Be able to provide proof that you are able to ensure compliance with these restrictions.

Disallowed Content

There are some types of messages that we can't allow on our platform, even if the recipient gives approval. 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.

1. Illegal Content. Content that is Illegal in the jurisdiction where the message recipient lives. For example - because United States federal laws prohibit the sale of recreational or medical cannabis and cannabis-derived CBD, those messages would not be allowed.

2. Harassment. Hate speech or harassment, or any communications from groups whose primary purpose is deemed to be spreading hate.

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

5. 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.

6. Malicious Activity & Content. Any content that is designed to intentionally evade security, throughput or other SignalWire filters. This also includes malicious content, such as malware or viruses.

Nonexclusive List of Examples of Disallowed Content

1. Social Marketing
2. Collections
3. Financial services, whether account notifications, marketing, collections or billing for:
    a. High-risk/subprime lending/credit card companies
    b. Auto loans
    c. Mortgages
    d. Payday loans
    e. Short-term loans
    f. Student loans
    g. Debt consolidation/reduction/forgiveness
4. Insurance
    a. Car Insurance
    b. Health Insurance
5. Gambling, Casino, and Bingo
6. Gift cards
7. Sweepstakes
8. Free prizes
9. Investment opportunities
10. Lead generation
11. Recruiting
12. Commission programs
13. Credit repair
14. Tax relief
15. Illicit or illegal substances (including Cannabis)
16. Work from home
17. Get rich quick
18. UGGS and RayBan campaigns
19. Phishing
20. Fraud or scams
21. Cannabis
22. Deceptive marketing

23. SHAFT: Sex, Hate/Harassment, Alcohol, Firearms or Tobacco related content
24. Any malicious activity that is designed to intentionally evade security, throughput or other SignalWire filters. This also includes malicious content, such as malware or viruses.

Monitoring

Today carriers use industry-leading spam containment vendors and monitor consumer complaints. These practices promote a sustainable model for healthy commercial texting, which is good for both consumers and message senders.

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).

Carriers monitor consumer complaints sent to this service for numbers on the 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 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.

Opt-Out Rate

Carriers track the opt-out rate on every source phone number that is active on their network. The daily opt-out rate on a phone number is defined as the total number of unique consumer phone numbers divided by the unique opted-out consumers that were sent messages within a 24-hour period.

If the daily opt-out rate on a sending phone number is 5% or greater, then the account is flagged for monitoring. An opt-out rate of 10% or greater on a sending phone number may result in immediate suspension of services.

Real-Time Content Analysis

Real-time analysis is used by carriers to identify if a message falls outside of the code of conduct or best practices.

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
MMA Best Practices
M3AAWG Best Practices
Telephone Consumer Protection Act (TCPA) Omnibus
Declaratory Ruling (FCC 15-72)
FTC Truth in Advertising
AT&T Code of Conduct
T-Mobile Code of Conduct