Sinch Voice: Messaging Best Practice Guidelines

These **Sinch Voice**[1] **Messaging Best Practices Guidelines** (these "Guidelines") are intended to provide general guidance and are proprietary information of Sinch Voice. These Guidelines provided for informational purposes only and Sinch Voice makes no warranties in these Guidelines. These Guidelines are not inclusive or exhaustive and are subject to change at Sinch Voice's discretion, at any time. Sinch Voice reserves the right in its sole discretion to remove or deny any traffic that does not comply with these Guidelines.

September 16, 2024

[1] Sinch Voice is the marketing name for Inteliquent, Inc. Inteliquent is a Sinch company.

TABLE OF CONTENTS

1.0 Introduction

The Sinch Voice messaging solution supports high-quality, high-integrity communications. Spam or unwanted messaging is forbidden. To protect consumers and the ecosystem from abuse, Sinch Voice enforces guidelines designed to promote best practices for exchange of messages.

The viability of the messaging ecosystem is dependent on Consumer perception of messaging as a trusted and convenient communication environment. These Guidelines are intended to preserve the credibility and utility of the ecosystem.

The objective of these Guidelines is to enable wanted messages and prevent unwanted or deceptive messages. While these Guidelines are intended to encourage correct behaviors, the spirit behind them is equally important. Message senders acting in bad faith to thwart or undermine the spirit of these policies should expect to experience penalties.

2.0 Enforcement

2.1 Policy Enforcement

Policy enforcement is performed at several points during message delivery including:

1. Sinch Voice Policy Management systems
2. Aggregator Policy Management systems (e.g., Sinch, Syniverse, Zipwhip)
3. Carrier Policy Management systems (e.g., T-Mobile, Verizon Wireless, AT&T Wireless)

2.2 Unregistered Non-Consumer (A2P) 10DLC Traffic

Sinch Voice does not support un-registered A2P 10DLC traffic.

3.0 Violations

Violations of guidelines may result in one or more of the following resolutions taken by Sinch Voice, aggregator or carrier:

1. Blocking of individual messages
2. Blocking of Telephone Numbers
3. Blocking of entire campaigns and/or brands
4. Blocking of NNIDs/SPIDs
5. Repeated violation may result in termination of messaging or other network services.

4.0 Definitions

Application to Person (A2P): Per the June 2023 version of the CTIA Guidelines, we now refer to A2P as **Non-Consumer messaging.** Messages sent from any non-consumer (business, organization, or agent of a business) business to a consumer. The definition does not require an actual application send the message, just that the messaging be a business to consumer communication. Some common use cases include two factor authentication (2FA), travel notifications, banking alerts, delivery notifications, customer care, etc. Non-Consumer (A2P) delivery methods are either via 8xx (Toll Free) messaging service or 10DLC (10 digit long code).

Blocklisting: Numbers that have sent repeated known SPAM/unwanted content are subject to automatic blocklisting without notification for up to 30 days. Multiple or repeat offenses may result in permanent blocklisting. Additionally, numbers that have been reported by industry partners for SPAM/unwanted content may also be subject to permanent blocklisting.

Consumer: An individual person who subscribes to specific wireless messaging services or messaging applications. *Consumers do not include agents of businesses, organizations, or entities that send messages to Consumers*. Consumers are natural persons with uniquely assigned telephone numbers (long codes i.e. local telephone numbers) that can be dialed. See the latest CTIA Guidelines for more information.

Fingerprinting: The process of extracting data points from identified SPAM content is known as "fingerprinting". Once message content has been fingerprinted as SPAM, all content found to be correlated to that fingerprint will be blocked in the future. Fingerprints do not expire or age out of existence.

MM4: MM4 is a 3GPP protocol for MMS service that covers the routing of an MMS from an originator MMS Relay/Server to a recipient MMS Relay/Server. MM4 is based on SMTP (email) protocol. MM4 is an extension of Internet Simple Mail Transport Protocol (SMTP) according to STD 10 (RFC 2821).

Multimedia Message Service (MMS): Facilitates group messaging and allows for the exchange of multimedia content between mobile devices including, video, pictures and audio.

Non-Consumer: A business, organization, or entity that uses messaging to communicate with Consumers. Examples may include, but are not limited to, large-to-small businesses, financial institutions, schools, medical practices, customer service entities, non-profit organizations, and political campaigns. See the CTIA Guidelines for more information.

Person to Person (P2P): Per the June 2023 version of the CTIA Guidelines, now referred to as **Consumer messaging**. *Consumer (P2P) messaging is sent by a Consumer to one or more Consumers and is consistent with typical Consumer operation (i.e., message exchanges are consistent with conversational messaging among Consumers).* Some Consumers utilize automation to assist in responding to communications. For example, a Consumer may direct their messaging service to autoreply to a phone call in order to inform the caller about the Consumer's status (e.g., "I'm busy" or "Driving now, can't talk"). Such use of automation to assist Consumers in their composition and sending of messages falls within the attributes of typical Consumer operation. In contrast, automation in whole or in part used by non-Consumers to facilitate messaging is not typical Consumer operation.

REST API: Application Programing Interface used to establish Messaging connectivity for sending and receiving messages and other service-related access.

Short Message Service (SMS): Commonly known as "text messaging," this is a service for sending and receiving messages of up to 160 characters to mobile devices. Longer messages will be fragmented into smaller message fragments. Maximum character length per message fragment varies depending on the character set used in the body of the message, whether GSM default alphabet or Unicode.

Short Message Peer-to-Peer (SMPP): SMPP is an open, industry standard Internet protocol designed to provide a flexible data communication interface for the transfer of SMS messages between External Short Messaging Entities (ESME), Routing Entities (RE) and Short Message Service Centers (SMSC).

Unwanted Messages: May include, but are not limited to, unsolicited bulk commercial messages (i.e., Spam); “phishing” messages intended to access private or confidential information through deception; other forms of abusive, harmful, malicious, unlawful, or otherwise inappropriate messages; and messages that require an opt-in but did not obtain such opt-in (or such opt-in was revoked).

5.0 Volumetric Limitations

5.1 Global Settings

Sinch Voice messaging customers will be limited on messaging volume as follows:

5.1.1 SMPP and MM4

- SMPP: 100 SMS messages per second (6,000 messages per minute) per bind
- MM4: 20 MMS messages per second per SMTP peer

These noted rates are subject to change.

5.1.2 REST API

- REST (REpresentational State Transfer)-based messages are managed the account level.

5.2 Source Number Settings (applicable to both SMS and MMS)

5.2.1 Consumer or Person-to-Person (P2P)

These rates are based on guidelines outlined in the CTIA Messaging Principles and Best Practices.

- 60 messages per minute from a single originating telephone number
- 100 distinct recipients/terminating telephone numbers per messages
- 1,000 messages per 24 hours from a single originating telephone number
- 1:1 ratio of outgoing to incoming messages per telephone number with some latitude in either direction 25 repetitive messages
- 1 telephone number assigned to or utilized by a single Consumer

5.2.2 Non-Consumer or Application-to-Person (A2P) using 8XX (Toll Free) and 10DLC (10 digit) telephone numbers

- Non-Consumer (A2P) enabled operator destinations (AT&T, Verizon, T-Mobile, US Cellular, etc.)
- No additional defined per single originating 8XX toll free number velocity cap, see global thresholds listed above.
- Depending on Non-Consumer (A2P) 10DLC Campaign registration with AT&T, TPS is based on approved campaign class (or use-case)
- T-Mobile manages Non-Consumer (A2P) 10DLC based on brand global EIN

6.0 Global Policies

Throughout these Policies and Best Practices, it is important to note that we draw on information from the CTIA Principles and Best Practices (https://www.ctia.org/the-wireless-industry/industry-commitments/messaging-interoperability-sms-mms). This document is the guiding force that both US P2P (Consumer) and A2P (Non-Consumer, including 10DLC) draw upon.

6.1 General Rules of Content

Message senders should take affirmative steps and employ tools that monitor and prevent Unwanted Message content, including content that:

1. Is unlawful, harmful, abusive, malicious, misleading, harassing, violent, obscene/illicit, or defamatory,
2. Is deceptive (e.g., phishing messages intended to access private or confidential information), including deceptive links,
3. Invades privacy.
4. Promotes illegal activity,
5. Causes safety concerns,
6. Incites harm, discrimination, hate or violence,
7. Intended to intimidate,
8. Includes malware,
9. Threatens Consumers,
10. Does not meet age-gating requirements,

6.2 Political Use Cases

Political messaging will be evaluated on a case-by-case basis. Such discretion will not be exercised with the intent of favor or disfavor of any political party or candidate.

Due to high volumes of consumer complaints, messages containing the following content are not appropriate and may be blocked by carriers if sent over either P2P or A2P (Tollfree/10DLC) messaging, **regardless of opt-in status**:

- Spoofing messages or snowshoed content across multiple numbers
- Data sharing between message senders
- Malicious content
- Phishing content

6.3 Group Messaging

Group Messaging Depending on the specific implementation, group messaging might utilize phone numbers that are typically not assigned to a unique individual, and their characteristics may be inconsistent with Consumer messaging. Therefore, depending on the particular characteristics of a service, Service Providers may require special arrangements to facilitate group messaging phone numbers (e.g., similar to Non-Consumer), such as the identification of group messaging phone numbers.

It is recommended that group messaging services:

- Have strong anti-abuse controls and mechanisms appropriate for systems with potentially large message distribution;
- Support the ability of any member to opt-out of the group at any time; and
- Employ mechanisms to prevent recursive group messaging and cyclical messaging involving more than one group (e.g., in which one group is a member of another group).

6.4 Inappropriate Use Cases / Disallowed Content

In general, messages containing certain content have created a high volume of consumer complaints, causing different use cases to be disallowed and leading to the removal of blocked traffic for US A2P (including 10DLC, short codes, and toll-free), regardless of opt-in status.

High-Risk Financial Services

- Payday Loans
- Short Term- High Interest Loans
- Auto Loans & Mortgage Loans from non-direct lenders.
- Student Loans
- Debt Collection
- Gambling/Sweepstakes
- Stock Alerts
- Cryptocurrency

Get Rich Quick Schemes

- Deceptive Work from Home Programs
- Risk Investment Opportunities
- Multi-Level Marketing

Job Postings

- Exceptions permitted if the message sender is the one doing the hiring

Debt Forgiveness

- Debt Consolidation
- Debt Reduction
- Credit Repair Programs

Controlled Substances

- Cannabis, CBD & Hemp Products
- All Schedule 1 & 2 drugs
- Tobacco and Vape

Other Disallowed use cases

- Phishing
- Pornography
- Profanity or Hate Speech
- Fraud or Scam

- Deceptive Marketing
- Lead Generation
- Referral or Reseller Campaigns

SHAFT (Sex, Hate, Alcohol, Firearms, Tobacco)

Age Gating: Alcohol, Firearms and Tobacco/Vape (as long as they do not contain CBD, Cannabis components) products may be conditionally approved with appropriate age-gating in place. All content must adhere to all appliable laws and support a functioning age-gate to comply with any age-restricted legal regulations. Non-acceptable age-gating functions include but is not limited to Yes or No only responses. The age-gating mechanism should include the date of birth verification during the consent opt-in of the consumer.

6.5 Additional Prohibited Practices

6.5.1 Snowshoe Messaging

Snowshoe sending is a technique used to send messages from more source phone numbers or short codes than are needed to support an application's function. This technique is often used to dilute reputation metrics and evade filters. Message Senders should not engage in Snowshoe Messaging. Service Providers should also take measures to prevent Snowshoe Messaging.

There may be cases where similar campaigns use different numbers. In that case, it is important that Message Senders identify their messages with a distinct brand and URL naming convention. If there is any doubt about campaign content, we suggest submitting use case proposals or questions to Sinch Voice's Messaging team.

6.5.2 Proxy Numbers

Message Senders might utilize a telephone number as a proxy number that functions as a relay point between possibly large sets of phone numbers and/or frequently changing phone numbers in certain wireless messaging use cases. For example, a driver for a ride-sharing service may need to communicate with a prospective passenger to confirm a pick-up location. The proxy telephone number functions as a conference call bridge telephone number, allowing the driver and passenger to communicate without either party having to reveal their personal telephone number. A 10-digit NANP telephone number used as a proxy is typically a means to connect two individuals, but proxy numbers are commonly reused in a way that may create volumes of messaging traffic that exceed typical Consumer operation. Given the use of proxy numbers to facilitate bulk messaging traffic among multiple 10-digit NANP telephone numbers, the proxy number qualifies as Non-Consumer (A2P) messaging traffic and may be subject to additional validation, vetting, and monitoring.

6.5.3 Spoofing Telephone Numbers

Message number spoofing includes the ability of a Message Sender to cause a message to display an originating number for the message that is not assigned to the Message Sender, or when a Message Sender originates a message through a Service Provider other than the Service Provider to which reply messages will be delivered or received. Message number spoofing should be avoided and should comply with all applicable laws.

7.0 Consumer (P2P) Best Practices

P2P messaging (or Consumer to Consumer messaging) is best defined in the CTIA Principles and Best Practices: "Consumer (P2P) messaging is sent by a Consumer to one or more Consumers and is consistent with typical Consumer operation (i.e., message exchanges are consistent with conversational messaging among Consumers). "

In P2P, auto-reply messaging is supported. Some Consumers utilize automation to assist in responding to communications. For example, a Consumer may direct their messaging service to autoreply to a phone call to inform the caller about the Consumer's status (e.g., "I'm busy" or "Driving now, can't talk"). Such use of automation to assist Consumers in their composition and sending of messages falls within the attributes of typical Consumer operation. In contrast, automation in whole or in part used by non-Consumers to facilitate messaging is not typical Consumer operation.

Non- Consumer (A2P) use-cases are prohibited.

8.0 Non-Consumer (A2P) Best Practices

8.1 Consumer Consent

The messaging ecosystem should operate consistent with relevant laws and regulations, such as the TCPA and associated FCC regulations regarding Consumer consent for communications. Regardless of whether these rules apply and to maintain Consumer confidence in messaging services, Non- Consumer (A2P) Message Senders should:

- Obtain a Consumer's consent to receive messages generally;
- Obtain a Consumer's express written consent to specifically receive marketing messages; and
- Ensure that Consumers have the ability to revoke consent.

Consent may vary upon on the type of message content exchanged with a Consumer.

The following table provides examples of the types of messaging content and the associated consent that should be expected. The examples below do not constitute or convey legal advice and should not be used as a substitute for obtaining legal advice from qualified counsel. Reference to "business" below is used as an example of a Non-Consumer (A2P) Message Sender. Individual Service Providers may adopt additional Consumer protection measures for Non-Consumer (A2P) Message Senders, which may include, for example, campaign pre-approval, Service Provider vetting, in-market audits, or Unwanted Message filtering practices that are tailored to facilitate the exchange of wanted messaging traffic.

Exhibit II: Types of Messaging Content & Associated Consent Principles		
Conversational	Informational	Promotional
Conversational messaging is a back- and-forth conversation that takes place via text. If a Consumer texts a business first and the business responds quickly with a single message, then it is likely conversational. If the Consumer initiates the conversation and the business simply responds, then no additional permission is expected.	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 needs to agree to receive texts for a specific informational purpose 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 (e.g., a coupon code to an informational text) may place the message in the promotional category. Before a business sends promotional messages, the Consumer should 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 only sent by a Consumer Two-way conversation	First message is sent by the Consumer or business One-way alert or two-way conversation	First message is sent by the business One-way alert
Message responds to a specific request	Message contains information	Message promotes a brand, product, or service 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 expected.	EXPRESS CONSENT The Consumer should give express permission before a business sends them a text message. Consumers may give permission over text, on a form, on a website, or verbally. Consumers may also give written permission.	EXPRESS WRITTEN CONSENT The Consumer should give express written permission before a business sends them a text message. Consumers may sign a form, check a box online, or otherwise provide consent to receive promotional text messages.

8.2 Clear and Conspicuous Calls-to-Action

A "Call-to-Action" is an invitation to a Consumer to opt-in to a messaging campaign. The Call-to-Action for a single-message program can be simple. The primary purpose of disclosures is to ensure that a Consumer consents to receive a message and understands the nature of the program.

Message Senders should display a clear and conspicuous Call-to-Action with appropriate disclosures to Consumers about the type and purpose of the messaging that Consumers will receive.

A Call-to-Action should ensure that Consumers are aware of: (1) the program or product description, (2) the telephone number(s) or short code(s) from which messaging will originate; (3) the specific identity of the organization or individual being represented in the initial message; (4) clear and conspicuous language about opt-in and any associated fees or charges; and (5) other applicable terms and conditions (e.g., how to opt-out, customer care contact information, and any applicable privacy policy).

Calls-to-Action and subsequent messaging should not contain any deceptive language, and opt-in details should not be obscured in terms and conditions (especially terms related to other services).

8.3 Consumer Opt-In

Message Senders should support opt-in mechanisms, and messages should be sent only after the Consumer has opted-in to receive them. Opt-in procedures reduce the likelihood that a Consumer will receive an Unwanted Message. It can also help prevent messages from being sent to a phone number that does not belong to the Consumer who provided that phone number (e.g., a Consumer purposefully or mistakenly provides an incorrect phone number to the Message Sender).

Depending upon the circumstances, a Consumer might demonstrate opt-in consent to receive messaging traffic through several mechanisms, including but not limited to:

- Entering a telephone number through a website.
- Clicking a button on a mobile webpage.
- Sending a message from the Consumer's mobile device that contains an advertising keyword.
- Initiating the text message exchange in which the Message Sender replies to the Consumer only with responsive information.
- Signing up at a point-of-sale (POS) or other Message Sender on-site location; or
- Opting-in over the phone using interactive voice response (IVR) technology.

While the Common Short Code Handbook is a separate document specific to the Common Short Code program, the Common Short Code Handbook has additional examples of opt-in consent that may be helpful to Message Senders.

Message Senders should also document opt-in consent by retaining the following data where

applicable:

- Timestamp of consent acquisition.
- Consent acquisition medium (e.g., cell-submit form, physical sign-up form, SMS keyword, etc.).
- Capture of experience (e.g., language and action) used to secure consent.
- Specific campaign for which the opt-in was provided.
- IP address used to grant consent.
- Consumer phone number for which consent to receive messaging was granted; and
- Identity of the individual who consented (name of the individual or other identifier (e.g., online user name, session ID, etc.)

8.4 Confirm Opt-In Confirmation for Recurring Messages

Message Senders of recurring messaging campaigns should provide Consumers with a confirmation message that clearly informs the Consumer they are enrolled in the recurring message campaign and provides a clear and conspicuous description of how to opt-out.

After the Message Sender has confirmed that a Consumer has opted-in, the Message Sender should send the Consumer an opt-in confirmation message before any additional messaging is sent.

The confirmation message should include:

(1) the program name or product description;

(2) customer care contact information (e.g., a toll-free number, 10-digit telephone number, or HELP command instructions);

(3) how to opt-out;

(4) a disclosure that the messages are recurring and the frequency of the messaging; and

(5) clear and conspicuous language about any associated fees or charges and how those charges will be billed.

Additional information can be found in:

https://api.ctia.org/wp-content/uploads/2023/05/230523-CTIA-Messaging-Principles-and-Best-Practices-FINAL.pdf

8.5 Consumer Re-Opt-In on Toll-Free Numbers

A Consumer may opt in to a Toll-Free A2P campaign by texting the word “UNSTOP” to the sender’s Toll-Free number. This keyword is not case sensitive and triggers opt-in only when sent as a single word.

Examples of valid re opt-ins:

- UNSTOP including variations such as unstop, Unstop or UNStop
- START

8.6 Single Opt-In per Campaign

Opt-ins are not transferable. A consumer opt-in to receive messages should not be transferable or assignable. A consumer opt-in should apply only to the campaign(s) and specific message sender for which it was intended or obtained.

8.7 Renting, Selling, or Sharing Opt-In Lists

Message senders should not use opt-in lists which have been rented, sold or shared to send messages. Message senders should create and vet their own opt-in lists.

8.8 Consumer Opt-Out

Opt-out mechanisms facilitate Consumer choice to terminate messaging communications, regardless of whether Consumers have consented to receive the message. Message Senders should acknowledge and respect Consumers' opt-out requests consistent with the following guidelines:

- Message Senders should ensure that Consumers have the ability to opt-out of receiving Messages at any time;
- Message Senders should support multiple mechanisms of opt-out, including phone call, email, or text; and
- Message Senders should acknowledge and honor all Consumer opt-out requests by sending one final opt-out confirmation message per campaign to notify the Consumer that they have opted-out successfully. No further messages should be sent following the confirmation message.
- Message Senders should state in the message how and what words effect an opt-out. Standardized "STOP" wording should be used for opt-out instructions, however opt-out requests with normal language (i.e., stop, end, unsubscribe, cancel, quit, "please opt me out") should also be read and acted upon by a Message Sender except where a specific word can result in unintentional opt-out. The validity of a Consumer opt-out should not be impacted by any de minimis variances in the Consumer opt-out response, such as capitalization, punctuation, or any letter-case sensitivities.

Examples of valid opt-out messages:

- STOP including variations such as Stop or STop
- Quit
- Cancel
- Unsubscribe
- End
- Opt me out

- Reference the following additional information: https://community.sinch.com/t5/SMS/Standard-opt-out-keywords-and-advanced-alternatives-for-USA-and/ta-p/14159

8.9 High Opt-Out Rate

Message senders who receive high volumes of opt-outs could be flagged and indicative of poor

sending practices. In the case that the daily opt-out rate is 5% or higher, the Toll-free carrier or other carriers may monitor the campaign. The carrier may reach out for campaign and opt-in details and/or suspend services of high opt-out rate flagged campaigns at its discretion, not to be unreasonably exercised.

"Daily opt-out rate" is the total number of subscribers who received a campaign's SMS divided by the number of opted out subscribers who received a campaign's SMS in a 24-hour period.

8.10 Maintaining and Updating Consumer Information

Message Senders should retain and maintain all opt-in and opt-out requests in their records to ensure that future messages are not attempted (in the case of an opt-out request) and Consumer consent is honored to minimize Unwanted Messages. Message Senders should process telephone deactivation files regularly (e.g., daily) and remove any deactivated telephone numbers from any opt-in lists.

8.11 Privacy and Security

Message Senders should address both privacy and security comprehensively in the design and operation of messaging campaigns. Sinch Voice is not responsible of liable for any security or breaches experienced by the Message Sender.

8.11.1 Maintain and Conspicuously Display a Clear, Easy-to-Understand Privacy Policy

Message Senders should maintain and conspicuously display a privacy policy that is easily accessed by the Consumer (e.g., through clearly labeled links) and that clearly describes how the Message Sender may collect, use, and share information from Consumers. All applicable privacy policies should be referenced in and accessible from the initial call-to-action. Message Senders also should ensure that their privacy policy is consistent with applicable privacy law and that their treatment of information is consistent with their privacy policy.

8.11.2 Implement Reasonable Physical, Administrative, and Technical Security Controls to Protect and Secure Consumer Information

Message Senders should implement reasonable security measures for messaging campaigns that include technical, physical, and administrative safeguards. Such safeguards should protect Consumer information from unauthorized access, use, and disclosure. Message Senders should conduct regular testing and monitoring to ensure such controls are functioning as intended.

8.11.3 Conduct Regular Security Audits

Message Senders should conduct either a comprehensive self-assessment or third-party risk assessment of privacy and security procedures for messaging campaigns on a regular

basis and take appropriate action to address any reasonably foreseeable vulnerabilities or risks.

8.12 Content

8.12.1 Prevention of Unlawful Activities or Deceptive, Fraudulent, Unwanted, or Illicit Content

Message Senders should use reasonable efforts to prevent and combat unwanted or unlawful messaging traffic, including spam and unlawful spoofing. Specifically, Message Senders should take affirmative steps and employ tools that can monitor and prevent Unwanted Messages and content, including for example content that: (1) is unlawful, harmful, abusive, malicious, misleading, harassing, excessively violent, obscene/illicit, or defamatory; (2) deceives or intends to deceive (e.g., phishing messages intended to access private or confidential information); (3) invades privacy; (4) causes safety concerns; (5) incites harm, discrimination, or violence; (6) is intended to intimidate; (7) includes malware; (8) threatens Consumers; or (9) does not meet age-gating requirements. Message Senders can also review the Common Short Code Handbook for further examples of Unwanted Message content.

Further, Message Senders should take steps to ensure that marketing content is not misleading and complies with the Federal Trade Commission's (FTC) Truth-In-Advertising rules.

8.12.2 Embedded Website Links

Message Senders should ensure that links to websites embedded within a message do not conceal or obscure the Message Sender's identity and are not intended to cause harm or deceive Consumers.

Where a web address or URL (Uniform Resource Locator) shortener is used, Message Senders should use a shortener with a web address and IP address(es) dedicated to the exclusive use of the Message Sender. Web addresses contained in messages as well as any websites to which they redirect should unambiguously identify the website owner (i.e., a person or legally registered business entity) and include contact information, such as a postal mailing address.

8.12.3 Embedded Phone Numbers

Messages should not contain phone numbers that are assigned to or forward to unpublished phone numbers, unless the owner (i.e., a person or legally registered business entity) of such phone numbers is unambiguously indicated in the text message.

8.13 Text-Enabling a Telephone Number for Non-Consumer (A2P) Messaging

An authentication and validation process should be used to verify the Message Senders' authority to enable Non-Consumer (A2P) messaging for a specific telephone number. Message Senders should only enable Non-Consumer (A2P) messaging with a telephone number that the Message Sender has been assigned by a provider of telecommunications or interconnected Voice over Internet Protocol (VoIP) services.

8.13.1 Toll-Free Campaign Registration

Sinch Voice requires registration of all Toll-Free (8xx) messaging campaigns) with the Toll-Free Gateway Provider before sending traffic. The information below is required for campaign review. The minimum review time is generally 4-5 business days, but in recent months, it may take substantially longer. Please check with the Sinch Voice team for current review delays. Use case information below should be submitted to MessagingUseCase@inteliquent.com

The information required for a Toll-Free Use Case Verification is as follows:

- 8XX Toll Free Number
- Use Case Summary
- Opt-In Process
- Message Examples
- Terms URL
- Privacy Policy

The Toll-Free use case verification works as follows:

1. Customer submits the VSR form to MessagingUseCase@inteliquent.com that can be found on the portal or by reaching out to IQ-ClientServices@sinch.com or MessagingUseCase@inteliquent.com
2. Sinch Voice reviews the form for any missing information or updates required.
3. Sinch Voice rejects the form back to the customer
   OR
   Sinch Voice submits the form to Toll-Free Gateway Provider for Verification review

4. The Toll-Free Gateway Provider rejects the form back to Sinch Voice which is communicated to the customer via the use case.
   OR
   The Toll-Free Gateway Provider verifies the Toll-Free number use case on their network

Verified traffic is subject to less blocking on The Toll-Free Provider Gateway and carrier networks which can result in Delivery Reports (DLRs) with status of 1152. Verified use cases still need to follow our Messaging Best Practices for opt-in consent and all other requirements.

Unverified traffic is subject to more spam blocking which can result in DLRs with status of 1160.

The Toll-Free Gateway Provider notes the following:

The messaging industry is changing the message volumes that can be sent over Restricted (previously called "unverified") and Pending (submitted for verification) Toll-Free numbers. Increased message filtering will also occur in addition to the new limits applied to both Restricted and Pending. If you've already verified your Toll-Free numbers, no further action is needed.

The following industry-wide thresholds for messaging sent over Restricted and Pending Toll-Free numbers:

Pending Verification

- *Daily limit: 2,000*
- *Weekly limit: 6,000*
- *Monthly limit: 10,000*

Registration is still required for all Toll-Free numbers when sending to Canada.

For the Canadian market, there are few additional rules for Toll-Free messaging (which, in reality, is good for all messaging):

- **Opt-out** rates must be below 1%
- **STOP reminders**: Campaigns must send stop language on the first and 5th message or once a month for continued customer awareness. However, sending it on every message is recommended.
- If a single number gets blocked with the Canadian carriers, please do not move traffic to another number.
- Messages should always identify who the sender of the message is.
- The number of messages sent to a subscriber should not exceed 10 in a month. If there is an expectation that the subscriber will receive multiple messages then that should be stated during the opt-in process
- Campaigns should support HELP, INFO, STOP as well as all French translations and send a bounce back in the corresponding language of the keyword
- Sinch Voice monitors on behalf of customers, but we encourage any issues to be reported to noc@inteliquent.com
- When a customer receives and MT with a link to a website, messages must also state that "Data rates may apply."

8.13.2 10DLC Campaign Registration

All business-to-consumer A2P 10DLC traffic must be registered with The Campaign Registry (TCR) to comply with Mobile Network Operator policies for the 10DLC program. The campaign registration process includes Brand registration (vetting application, if desired by the customer) followed by Campaign registration.

All campaigns are vetted reviewing the following information to confirm validity:

- Brand information and online presence
- Campaign Description & Use Case
- Call-to-Action / Message Flow

- Sample messages containing:
    - Brand name, website, call to action, opt-out/help language
- Confirming content does not fall into disallowed content
- Confirming MT, HELP and STOP flow and template messages
    - Opt-in (initial message): Program/brand name, msg frequency, pricing disclosure, help info, stop info
    - Help response: Program/brand name, contact info (phone number, email and/or support website URL)
    - Stop response: Program/brand name, confirmation that user has unsubscribed and will not receive any more messages

The campaign description should clearly explain for what purpose the messaging is being used by the company. For example, if being used for customer care/account notification:

> Description: Communication with customers for account updates, delivery notifications and issue resolution.

The sample messages should be specific, detailed messages representing the type of messages that would be send from the campaign. For example, if being used for customer care:

- Sample Message 1: Thank you for contacting [Company Name]. We will get back to as soon as possible. Reply STOP to opt-out.
- Sample Message 2: HI [name]. [Company Name], Just reaching out to remind you that your invoice payment due date is June 1. Reply STOP to opt-out
- Sample Message 3: Hey [name], great news! Your [Company Name] order is on its way! Reply STOP to opt-out
- Sample Message 4: Hi [name]. We are sorry to hear that you're having an issue with your [Company Name] product. Please respond with additional information for our service representatives to help resolve this for you. Reply STOP to opt-out

After the Brand and CampaignID values are registered with TCR, Sinch Voice will allow for TN SMS and MMS feature provisioning on the approved A2P 10DLC Campaign ID.

Customers should register directly with TCR at the link
https://csp.campaignregistry.com/dashboard

Failure to comply with these Guidelines may result in any of the following:

- Downgrade in message service class
- Suspension or termination of specific campaign, 10DLC numbers or message sender

Unidentified or unknown message senders may result in 10DLC P2P class of service anti-spam policies being used.

Message Classes and policies may be adjusted with notice based on observed messaging campaign characteristics, such as subscriber complaints and unsubscribe requests.

8.14 Political Messaging

Political campaigns need to follow all opt-in / consent guidelines outlined in the CTIA page:

Political Text Messaging: Engaging and Organizing Voters While Protecting Consumers: https://www.ctia.org/news/political-text-messaging-engaging-and-organizing-voters-while-protecting-consumers

For 10DLC, Campaign Verify registration is required. For short codes or toll-free, Campaign Verify registration and vetting is highly recommended, but not required. The latest requirements for political entities can be found at the Campaign Verify website: https://www.campaignverify.org/.

Campaign Verify helps protect that campaign and/or political organization from any spoofing by verifying information about the organization. Carriers also require this extra vetting step.

In short political campaigns should adhere to the following:

- Campaign must be on a dedicated application address
- For 10DLC, vetting must be confirmed through Campaign Verify (www.campaignverify.org) with a Campaign Verify Token (which applies to all 10DLC political campaigns).

Political campaigns should abide by the:

M^{3}AAWG Mobile Messaging Best Practices for Political Programs Best Practices.

https://politicalmessaging.com/

9.0 Technical Message Specifications

9.1 Message Content Length

- UCS-2 (16 bit) = 70 character maximum. For longer multipart messages, a User Data Header (UDH) is added to the message to instruct the receiving device on how to reassemble the message, resulting in a maximum of 67 characters for the body of the message.
- Latin1 (8 bit) = 140 character maximum. For longer multipart messages, a User Data Header (UDH) is added to the message to instruct the receiving device on how to reassemble the message, resulting in a maximum of 134 characters for the body of the message.
- GSM7 (7 bit) = 160 character maximum. For longer multipart messages, a User Data Header (UDH) is added to the message to instruct the receiving device on how to reassemble the message, resulting in a maximum of 153 characters for the body of the message.
- Any message segment which has been broken up from a single message due to length will be treated as a single message as will messages to multiple recipients.

9.2 MMS Specific Policies

9.2.1. File Size

Maximum file size: operators support different maximum file attachment sizes. Please see carrier breakout below per size restriction.

AT&T:

- If the media is less than 1 MB, then it will PASS-ON to AT&T and no message resizing is done.
- If media is more than 1 MB and less than 3 MB, then Sinch Voice will do message resizing and then deliver the resized media/message to AT&T.
- If media is over 3 MB, then Sinch Voice/ULC will drop the message.
- AT&T will accept media up to 1 MB.

Verizon:

- Verizon will accept media up to 1.7MB.
- If media over 1.7 MB will be dropped by the carrier relay
- No message resizing will be done by the carrier relay if destination is Verizon.

T-Mobile/Sprint

- TMO will accept media up to 3 MB.
- If media over 3 MB will be dropped in carrier transit.
- No message resizing will be done by the carrier relay if destination is TMO or Sprint.

9.2.2 File Types

Below is a list of currently supported file types. File types outside of this list are not supported and will be rejected.

.

File Type	Extension
audio/3gpp	.3gp
audio/amr	.amr
audio/amr	.3ga
audio/mp4	.m4a
audio/mp4	.m4p
audio/mp4	.m4b
audio/mp4	.m4r
audio/mpeg	.mp3
audio/wav	.wav
image/bmp	.bmp
image/bmp	.dib
image/gif	.gif
image/jpeg	.jpg
image/jpeg	.jpeg
image/png	.png
video/3gpp	.3gp
video/h263	.h263
video/h264	.h264
video/mp4	.mp4
video/mp4	.m4v

10.0 Resources

This section includes links to industry resources that may be helpful as a message sender starts to craft messaging content. Messages should follow guidance from these resources, otherwise messages may be blocked.

CTIA Messaging Principles and Best Practices (Updated 05/2023)
https://api.ctia.org/wp-content/uploads/2023/05/230523-CTIA-Messaging-Principles-and-Best-Practices-FINAL.pdf

CTIA Keeping Political Text Messaging Spam-Free:
https://politicalmessaging.com/

CTIA Political Text Messaging: Engaging and Organizing Voters While Protecting Consumers
https://www.ctia.org/news/political-text-messaging-engaging-and-organizing-voters-while-protecting-consumers

CTIA Messaging Security Best Practices
https://www.ctia.org/the-wireless-industry/industry-commitments/messaging-security-best-practices

Campaign Verify – a non-partisan, nonprofit service for US political campaigns, parties, and PACs to verify their identity.
https://www.campaignverify.org/

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

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

M3AAWG Best Practices
https://www.m3aawg.org/documents/en/m3aawg-mobile-messaging-best-practices-for-service-providers-0

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