Messaging Best Practices

Non-Consumer Application to Person (A2P) message traffic includes, but is not limited to, messaging to and from large-to-small businesses, entities, and organizations. For example, Non-Consumer (A2P) messages may include messages sent to multiple Consumers from businesses or their agents, messages exchanged with customer service response centers, service alerts and notifications (e.g., fraud, airline), and machine-to-machine communications. Non-Consumer (A2P) Message Senders may also include financial service providers, schools, medical practices, customer service entities, non-profit organizations, and political campaigns.

Best Practices

Message Senders should:

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

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

Message Senders Should Provide 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.

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.

Message Senders Should Provide 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:

- the program or product description;
- the telephone number(s) or short code(s) from which messaging will originate;
- the specific identity of the organization or individual being represented in the initial message;
- clear and conspicuous language about opt-in and any associated fees or charges;
- 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).

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.)).

Confirm Opt-In 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.

Apply One Opt-In per Campaign

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.

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.
- 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.

Renting, Selling, or Sharing Opt-In Lists

Message Senders should not use opt-in lists that have been rented, sold, or shared to send messages. Message Senders

should create and vet their own opt-in lists.

Maintain and Update 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.

Privacy and Security

Message Senders should address both privacy and security comprehensively in the design and operation of messaging campaigns.

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.

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.

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.

Message Content

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:

- is unlawful, harmful, abusive, malicious, misleading, harassing, excessively violent, obscene/illicit, or defamatory;
- deceives or intends to deceive (e.g., phishing messages intended to access private or confidential information);
- invades privacy;
- causes safety concerns.
- incites harm, discrimination, or violence;
- is intended to intimidate.
- includes malware.
- threatens Consumers; or
- does not meet age-gating requirements.

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.

Version 01.05122025