Messaging Principles and Best Practices

May 2023

Table of Contents

1 Executive Summary

The Messaging Principles and Best Practices (Principles and Best Practices) are a set of voluntary best practices developed by CTIA's member companies throughout the wireless messaging ecosystem.

Messaging's popularity is largely attributable to its status as a trusted and convenient communications environment. These Principles and Best Practices are intended to reflect the wireless industry's efforts to preserve the trust in and utility of Wireless Providers' messaging services and help protect Consumers from Unwanted Messages. They identify parameters for facilitating the exchange via transmission, storage, and retrieval (exchange) of messages via Wireless Provider messaging networks.

Throughout these Principles and Best Practices, messages are categorized as either Consumer or Non-Consumer messaging depending on the Message Sender. The prior version of these Principles and Best Practices used the terms "Consumer (P2P)" and "Non-Consumer (A2P)." Some Wireless Providers may still use the legacy terms as part of their efforts to support a trusted messaging environment. The current definitions for Consumer and Non-Consumer are included in Section 3.3.

As explained in the definitions for these terms in Section 3.3, if the Message Sender is a business, organization, or other entity – or an agent, representative, or other individual acting on behalf of a business, organization, or other entity – the messaging is considered Non-Consumer. There are specific Principles and Best Practices that apply to Consumer messaging and others that apply to Non-Consumer messaging (e.g., Non-Consumers are expected to obtain a Consumer's consent before sending them messages).

The objectives of this document are to support a robust and dynamic wireless messaging community where:

- Consumers can exchange wanted messages with other Consumers;
- Message Senders and Consumers can exchange wanted messages; and
- Consumers are protected from Unwanted Messages, in conformity with applicable laws and regulations, such as the United States' Telephone Consumer Protection Act (TCPA) and the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act).

2 Scope

2.1 Purpose

The Principles and Best Practices are intended primarily for entities operating in the wireless messaging ecosystem to facilitate innovation and the use of wireless messaging while protecting Consumers from Unwanted Messages. The Principles and Best Practices may also help inform Consumers about wireless messaging services and anyone with an interest in the wireless messaging ecosystem.

These Principles and Best Practices represent an important further step in the wireless industry's effort to support new uses and business opportunities in wireless messaging services while maintaining protections for Consumers from Unwanted Messages. In particular, these Principles and Best Practices are intended to demonstrate Wireless Providers' efforts to balance the exchange of messaging traffic for, among other reasons, public interest purposes – including for example political, educational, emergency, and non-profit purposes – while continuing to protect Consumers from Unwanted Messages. By establishing clear parameters and guidelines, these Principles and Best Practices encourage Message Senders to maintain Consumer trust and confidence in Consumer services and support the adoption of innovative Non-Consumer services.

This version of the Principles and Best Practices replaces the 2019 CTIA Messaging Principles and Best Practices in order to further clarify expectations among wireless messaging ecosystem stakeholders for identifying Consumer and Non-Consumer messaging (as defined in Section 3.3) and establish clear guidelines for Non-Consumer messages.

Although the specific technical and operational details required for Service Provider implementation are beyond the scope of this document, the Principles and Best Practices acknowledge that Service Provider implementation will be an ongoing and iterative process that continues to evolve as new use cases arise. These Principles and Best Practices are meant to supplement, and not replace, CTIA's Common Short Code Monitoring Handbook.

In addition to these Principles and Best Practices, Non-Consumers should consult CTIA's Messaging Security Best Practices, which describe security-related best practices that Message Senders, Service Providers, and other entities participating in the wireless messaging ecosystem may use to address common threat vectors that can undermine Consumers' trust in the wireless messaging ecosystem.

2.2 Wireless Messaging Services

The Principles and Best Practices primarily address wireless messaging services that use 10-digit telephone numbers assigned from the NANP as the unique identifier for the sender and/or recipient(s) of individual or group messages. Generally, wireless

messages are exchanged between 10-digit NANP telephone numbers via Wireless Providers' messaging networks. These messaging services include:

- Short Message Service (SMS);
- Multimedia Messaging Service (MMS); and
- Rich Communications Services (RCS).

As described in Section 5.5 below, a five- or six-digit number known as a short code can also be used to exchange wireless messages via Wireless Providers' messaging networks. While these Principles and Best Practices should be interpreted consistent with CTIA's Common Short Code Monitoring Handbook, Message Senders that use a common short code (CSC) should adhere to the terms of those services as described in the Common Short Code Monitoring Handbook and individual wireless providers' terms of use.

The messaging ecosystem also includes cloud-based services that require the use of a separate messaging client (e.g., an app) that is distinct from and does not interoperate with Wireless Providers' messaging networks. These Principles and Best Practices are intended to apply to messaging services that only interoperate between cloud-based platforms and Wireless Providers' messaging networks using the applicable services, such as SMS, MMS, or RCS.

2.3 Scope, Limitations, & Disclaimer of Legal Guidance or Advice

CTIA's Principles and Best Practices do not constitute or convey legal advice and should not be used as a substitute for obtaining legal advice from qualified counsel. Use of and access to the Principles and Best Practices or any of the links contained herein do not create an attorney-client relationship with CTIA and the user.

Messaging services may be subject to a number of legal requirements, including for example those established under the TCPA; the CAN-SPAM Act; the Communications Act of 1934, as amended; the Federal Trade Commission Act; and implementing regulations and decisions adopted by the Federal Communications Commission and Federal Trade Commission.[1] Anyone using these Principles and Best Practices should consider obtaining legal and regulatory advice prior to taking any action related to the use of messaging services.

As a set of voluntary best practices, CTIA's Principles and Best Practices do not impose, prescribe, or require contractual or technical implementation on messaging ecosystem stakeholders, including Service Providers. Due to contractual, technical, or other practical factors, methods of implementing the Principles and Best Practices may vary among stakeholders. Stakeholders may choose to implement modified and additional requirements through their individual guidelines, policies, and contracts.

[1] *See, e.g.*, FCC, Petitions for Declaratory Ruling on Regulatory Status of Wireless Messaging Service, Declaratory Ruling, 33 FCC Rcd 12075 (2018); FCC, Text-Enabled Toll Free Numbers, Declaratory Ruling and Notice of Proposed Rulemaking, 33 FCC Rcd 2438 (2018).

3 Wireless Messaging Ecosystem

3.1 Background

In the late 1990s, wireless text messaging evolved to include two-way Consumer-to-Consumer traffic using 10-digit NANP telephone numbers. Wireless Providers' messaging systems were not interoperable – a subscriber could only communicate with other subscribers of the same Wireless Provider. In the early 2000s, CTIA established the *SMS Interoperability Guidelines*, which provided industry standards for SMS interoperation among mobile networks. Today, wireless messaging services have become a convenient and trusted communication tool for Consumers and, increasingly, enterprise users.

In the early 2000s, CTIA and other messaging ecosystem stakeholders developed the short code platform (i.e., five- or six-digit codes) to enable the appropriate use of bulk wireless messages (e.g., wireless messaging campaigns). Wireless Providers' combination of upfront vetting and ongoing auditing allows high-volume messaging campaigns while minimizing the risk that short codes will be used to distribute Unwanted Messages.

In 2009 and again in 2011, CTIA and messaging ecosystem stakeholders expanded the *SMS Interoperability Guidelines* to guide how non-mobile networks and cloud-based services could exchange SMS message traffic with mobile wireless networks. In 2014, CTIA and messaging stakeholders also revised the *SMS Interoperability Guidelines* to account for group messaging and text-enabled toll-free telephone numbers. As noted above, this version of the Principles and Best Practices replaces the 2019 CTIA Messaging Principles and Best Practices, which also replaced the *SMS Interoperability Guidelines*.

These efforts have shared a common goal of maintaining and enhancing a dynamic, competitive wireless messaging ecosystem while protecting Consumers from Unwanted Messages.

3.2 The Evolving Wireless Messaging Ecosystem

Messaging to 10-digit NANP telephone numbers has enabled Consumers to communicate generally with each other and with organizations in a low-volume, conversational manner. The wireless messaging ecosystem has strived to enable such low-volume, Consumer-oriented communications while simultaneously seeking to inhibit Unwanted Messages from reaching Consumers.

Messaging's popularity among Consumers is largely attributable to its status as a trusted and convenient wireless communications environment. Messaging is also an increasingly attractive platform to reach Consumers because of its broad adoption by Consumers and Consumers' ability to retrieve messages when convenient and to store them as desired.

In addition to well-established short code services, the Non-Consumer messaging ecosystem today includes two-way messaging traffic from 10-digit NANP telephone numbers. This messaging traffic may feature diverse characteristics (e.g., low or high volumes, balanced or imbalanced ratios of outgoing to incoming messages) and may serve conversational, informational, or promotional purposes. Regardless of the traffic's characteristics or purpose, these advances pose threats to Consumers if Unwanted Messages negatively impact the role of messaging as a trusted and convenient wireless communications medium. To protect Consumers from Unwanted Messages, Service Providers deploy filters and other tools that limit messaging traffic bearing the characteristics of Unwanted Messages. Section 7 of these Principles and Best Practices describes some of the principles that messaging ecosystem stakeholders should utilize to contain Unwanted Messaging traffic.

3.3 Messaging Ecosystem Roles

The messaging ecosystem comprises many stakeholders working together to create, route, deliver, store, retrieve, and consume messages.[2]

3.3.1 **Consumer**

A *Consumer* is an individual person who subscribes to specific wireless messaging services or messaging applications. **Consumers do <u>not</u> include agents, representatives, or any other individuals acting on behalf of Non-Consumers, including businesses, organizations, political campaigns, or entities that send messages to Consumers.**

3.3.2 **Non-Consumer**

A *Non-Consumer* is a business, organization, or entity that uses messaging to communicate with Consumers. **Examples include, but are not limited to, large-to-small businesses, financial institutions, schools, medical practices, customer service entities, non-profit organizations, and political campaigns. Non-Consumers also include agents, representatives, or any other individuals acting on behalf of Non-Consumers.**

3.3.3 **Wireless Facilities-Based Service Providers (Wireless Providers)**

Wireless Providers own and operate radio, telephone, and data networks and offer Consumers a wide variety of wireless communications products and services, including wireless messaging services such as SMS, MMS, and RCS.

3.3.4 **Mobile Virtual Network Operators (MVNOs)**

MVNOs are wireless Service Providers that do not own the network infrastructure over which they provide services. Instead, MVNOs resell network services maintained by one or more Wireless Providers.

[2] As noted above, the prior version of these Principles and Best Practices used the terms "Consumer (P2P)" and "Non-Consumer (A2P)." Some Wireless Providers may still use the legacy terms as part of their efforts to support a trusted messaging environment. The current definitions for Consumer and Non-Consumer are included in Section 3.3.

3.3.5 **Cloud-Based Providers**

Cloud-Based Providers enable services like voice and messaging to end-users using over-the-top IP connectivity or through interoperability with wireless carrier-networked services, including wireless messaging. Some Cloud-Based Providers offer an API to access wireless services, while others offer standalone applications.

3.3.6 **Inter-Carrier Vendors (ICVs)**

Also called Hub Providers, *ICVs* act as hubs to facilitate interoperability by transporting messaging traffic between multiple Wireless Providers and Cloud-Based Providers.

3.3.7 **Connection Aggregators**

Connection Aggregators offer a variety of value-added services to enterprise customers, including messaging connectivity with multiple Wireless Providers. Unlike ICVs, Connection Aggregators do not typically support inter-carrier peering traffic.

3.3.8 **Competitive Local Exchange Carriers (CLECs)**

In the messaging ecosystem, *CLECs* provide 10-digit NANP telephone numbers and traffic routing services to Cloud-Based Providers.

3.3.9 **Registrars**

Registrars operate databases of telephone numbers and databases of the associated Communications Provider or Providers enabling wireless messaging service to those 10-digit NANP telephone numbers (e.g., CLEC, Wireless Provider, Cloud-Based Provider). The databases establish a record of 10-digit NANP telephone number resources used to support the effective exchange of wireless messages. Registrars' customers include CLECs, Wireless Providers, ICVs, Cloud-Based Providers, and enterprises.

3.3.10 **Network Security Vendors**

Network Security Vendors provide solutions that enable Wireless Providers, Cloud-Based Providers, and ICVs to identify Unwanted Messaging traffic. These solutions deliver a variety of network security features, including spam containment and management.

3.3.11 **Service Providers**

Service Providers refers to any of the parties identified in Section 3.3 that offer messaging services or messaging-related services to Consumers or Non-Consumers using 10-digit NANP telephone numbers or short codes, including Wireless Providers, MVNOs, Cloud-Based Providers, and CLECs.

3.3.12 **Message Sender or Sender**

A *Message Sender* or *Sender* is any Service Provider or Non-Consumer that originates or transmits message traffic.

3.3.13 **Unwanted Messages**

Unwanted Messages (or *Unwanted Messaging*) may include 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; messages that required an opt-in but

did not obtain such opt-in (or such opt-in was revoked); and unwanted content noted in Content (Section 5.3).

4 Consumer / Non-Consumer Traffic Classification

4.1 Consumer Messaging

Consumer messaging is sent by a Consumer to one or more Consumers. Consumer messaging is uniquely originated from a single 10-digit NANP telephone number or chosen at the direction of the Consumer to a limited number of unique Consumer recipients. Consumer messaging is generally conversational, and an incoming message typically generates a response from the recipient. Consumer messaging does not involve substantially repetitive messages or exhibit characteristics of Unwanted Messaging traffic.

4.1.1 What is Typical Consumer Operation?

Exhibit I outlines the attributes of typical Consumer operation. These attributes are illustrative of (but do not determine whether messaging constitutes) Consumer messaging.[3] To determine whether messaging traffic qualifies as Consumer or Non-Consumer messaging traffic, Message Senders should review Sections 3.3.1 (Consumer), 3.3.2 (Non-Consumer), 4.1 (Consumer Messaging), and 4.2 (Non-Consumer Messaging).

Exhibit I Attributes of Typical Consumer Operation

In addition to being from a Consumer to one or more Consumers, Consumer messaging generally will feature the following attributes.

	ATTRIBUTE	NOTES
Throughput	15 to 60 messages per minute	A Consumer is typically not able to originate or receive more than about one message per second.
Volume	1,000 per day	Only in unusual cases do Consumers send or receive more than a few hundred messages in a day. A Consumer also cannot typically send or receive messages continuously over a long period of time.
Unique Sender	1 telephone number assigned to or utilized by a single Consumer	A single Consumer typically originates messages from a single telephone number.
Unique Recipients	100 distinct recipients/telephone numbers per message	A Consumer typically sends messages to a limited number of recipients (e.g., 10 unique recipients).

[3] For example, Non-Consumers increasingly use messaging technologies that enable them to easily send different types of messaging content to Consumers (e.g., conversational messaging). While this messaging traffic may satisfy the throughput, volume, and balance thresholds that are consistent with typical consumer operation, it would qualify as Non-Consumer messaging traffic because it is sent by a Non-Consumer (see Section 4.2).

Balance	1:1 ratio of outgoing to incoming messages per telephone number with some latitude in either direction	Consumer messages are typically conversational. An incoming message typically generates a response from the recipient.
Repetition	25 Repetitive Messages	Consumer messages are uniquely originated or chosen at the direction of the Consumer to unique recipients. Typical Consumer behavior is not to send essentially or substantially repetitive messages.

4.1.2 **Consumer Messaging Automation**

Some Consumers utilize automation to assist in responding to communications. For example, a Consumer may direct their messaging service to auto-reply 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 a Non-Consumer to facilitate messaging is not typical Consumer operation.

4.2 Non-Consumer Messaging

Non-Consumer messaging is sent by or to a Non-Consumer. Non-Consumer message traffic includes, but is not limited to, messaging to and from large-to-small businesses, entities, and organizations, including political campaigns. For example, Non-Consumer messages may include messages sent to multiple Consumers from a business or its agents, messages exchanged with a customer service response center, service alerts or notifications (e.g., fraud, airline), and machine-to-machine communications. Non-Consumer Message Senders also include financial service providers, schools, medical practices, customer service entities, non-profit organizations, and political campaigns or organizations. Specifically, such Message Senders should adhere to the Non-Consumer Best Practices as described in this document (see Section 5).

Protecting Consumers from Unwanted Messages, particularly from high-volume messaging traffic, is a key consensus-based goal among messaging ecosystem stakeholders. Having clear parameters around Consumer traffic will help facilitate the continued deployment of Non-Consumer services consistent with protecting networks and Consumers. Individualized arrangements and close collaboration among messaging ecosystem stakeholders creates an environment for the successful deployment of Non-Consumer messaging.

5 Non-Consumer Best Practices

5.1 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 Message Senders are expected to:

- 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.

The table below provides examples of the types of messaging content and the associated level of consent. 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.

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 Non-Consumer first and the Non-Consumer responds quickly with a single message, then it is likely conversational. If the Consumer initiates the conversation and the Non-Consumer simply responds, then no additional permission is expected.	Informational messaging is when a Consumer gives their phone number to a Non-Consumer 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 Non-Consumer 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 Non-Consumer sends promotional messages, the Consumer should agree in writing to receive promotional texts. Non-Consumers 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 Message responds to a specific request	First message is sent by the Consumer or Non-Consumer One-way alert or two-way conversation Message contains information	First message is sent by the Non-Consumer One-way alert 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 Non-Consumer only responds with relevant information, then no verbal or written permission is expected.	EXPRESS CONSENT The Consumer should give express permission before a Non-Consumer 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 Non-Consumer sends them a text message. Consumers may sign a form, check a box online, or otherwise provide consent to receive promotional text messages.

Individual Service Providers may adopt additional Consumer protection measures for Non-Consumer 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.

5.1.1 **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: (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).

5.1.2 **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.)).

5.1.2.1 **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.

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.

5.1.2.2 **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.

5.1.3 **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.

5.1.4 **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.

5.1.5 **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.

5.2 Privacy and Security

Message Senders should address both privacy and security comprehensively in the design and operation of messaging campaigns. Additional security guidelines and best practices are described further in the Messaging Security Best Practices.[4]

5.2.1 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.

5.2.2 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.

5.2.3 Conduct Regular Security Audits

Message Senders should regularly conduct a comprehensive 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.

5.3 Content

5.3.1 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-

[4] The Messaging Security Best Practices include, but are not limited to, best practices to prevent or address: (1) general security threats; (2) threats from messages that originate via email; (3) the misuse of disposable telephone numbers and free text-enabled telephone numbers; and (4) compromised API credentials or systems.

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.

5.3.2 **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 (i.e., Uniform Resource Locator (URL)) 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.

5.3.3 **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.

5.4 Text-Enabling a Telephone Number for Non-Consumer Messaging

An authentication and validation process should be used to verify the Message Senders' authority to enable Non-Consumer messaging for a specific telephone number. Message Senders should only enable Non-Consumer 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.

5.5 Other Non-Consumer Messaging Best Practices

5.5.1 **Shared Telephone Numbers and Short Codes**

The use of shared telephone numbers or short codes among multiple persons, businesses, entities, or organizations may require special arrangements between Message Senders and Service Providers. "Sub-aggregating" a single telephone number or short code with multiple Message Senders also may require special arrangements between Message Senders and Service Providers. In instances where shared number use is approved, all Message Senders operating on a shared number should be documented and available, if required through special arrangements between Message Senders and Service Providers.

5.5.2 **Snowshoe Messaging**

Message Senders should not engage in Snowshoe Messaging, which is a technique used to spread messages across many sending phone numbers or short codes. Service Providers should also take measures to prevent Snowshoe Messaging. Additional best

practices addressing Snowshoe Messaging can be found in the Messaging Security Best Practices.

Messaging use cases that require the use of multiple numbers to distribute "similar" or "like" content may require special arrangements between Message Senders and Service Providers.

5.5.3 **Grey Routes**

Message Senders should not utilize Grey Routes to send messages. A Grey Route is a setting, method, or path that is not authorized by Service Providers for Non-Consumer messages. Messages are either Consumer or Non-Consumer in accordance with these Principles and Best Practices and subject to individual Service Providers' policies and arrangements. Additional best practices addressing Grey Routes can be found in the Messaging Security Best Practices.

5.5.4 **Common Short Codes**

Common short codes are non-NANP addresses of 5 or 6 digits typically used by businesses, entities, or organizations for high-volume communications with Consumers (e.g., airline flight delays, banking account alerts, shipping company delivery notifications, school delays). The short code platform was developed to accommodate higher-volume SMS traffic by providing upfront Consumer protections from Unwanted Messaging traffic and procedures to ensure appropriate use of the platform.

In the United States, the Common Short Code Administration (CSCA) operates the cross-carrier short code registry. The CTIA Short Code Monitoring Handbook offers best practices and other guidelines for conducting Non-Consumer messaging campaigns using short codes.

In Canada, the Canadian Wireless Telecommunications Association (CWTA) administers short code assignments through its txt.ca website. The Canadian Common Short Code Application Guidelines publication offers best practices and other guidelines for short code campaigns in the Canadian marketplace.

5.5.5 **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. Another example is a service that allows a user to establish a single telephone number with the ability to relay calls and messages to any of several other telephone numbers held by the user.

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 high volumes of messaging traffic. 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 messaging traffic and may be subject to additional validation, vetting, and monitoring by Service Providers. Although Consumer group messaging services may use proxy numbers and display some characteristics of Non-Consumer messaging, special consideration can be given for these group messaging services, as discussed in Section 6.1 below.

5.5.6 **Text-Enabled Toll-Free Telephone Numbers**

Toll-free telephone numbers are a subset of NANP telephone numbers that use the following numbering plan area codes (NPAs): 800, 888, 877, 866, 855, and 844. NPA 833 is tentatively planned for the future. While toll-free numbers have generally supported only voice calling, the messaging ecosystem has evolved to allow use of a toll-free telephone number as the identifier for wireless messaging services.

To uphold the integrity of toll-free telephone numbers, to provide transparency to Responsible Organizations (Resp Orgs) that manage the use of toll-free numbers for voice services, and to protect Consumers from Unwanted Messages from toll-free numbers, Message Senders should operate in accordance with the following guidelines:

5.5.6.1 **Authority to Text-Enable Rests with the Toll-Free Voice Subscriber**

The toll-free subscriber who is the holder of record of a toll-free number for voice services has the sole authority to control additional services associated with that toll-free number. Only toll-free numbers that are currently reserved or in working status for the benefit of a toll-free number voice subscriber should be enabled for messaging.[5]

5.5.6.2 **Transparency to Resp Orgs**

To provide transparency to Resp Orgs and other Service Providers regarding toll-free numbers that are wireless messaging-enabled, any process for provisioning messaging associated with a toll-free number should allow or provide for synchronization with a registry or registries that provide a comprehensive record of text-enabled toll-free numbers and associated toll-free number subscribers. In addition, registries should be operated consistent with the principles in Section 6.3 below.

5.5.6.3 **Special Considerations for Shared-Use Toll-Free Telephone Numbers**

For the benefit of a toll-free number voice subscriber, message enablement of a toll-free number should account for any shared-use arrangements that are part of the voice service associated with the toll-free number. In the case of shared-use toll-free numbers, the toll-free voice Service Provider should be treated as the toll-free

[5] *See*, FCC, Text-Enabled Toll Free Telephone Numbers, Declaratory Ruling and Notice of Proposed Rulemaking, 33 FCC Rcd 6551 (2018).

subscriber to uphold the integrity of the toll-free number and protect subscribers of a toll-free voice service that terminates voice telephony traffic to more than one subscriber. Such shared-use arrangements include, but are not limited to, geographic-based and time-of-day-based sharing.

6 Special Use Cases

6.1 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).

6.2 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. Message number spoofing may also require special arrangements between Message Senders and Service Providers.

6.3 Registries

To achieve impartiality with respect to number registration, Registrars should commit to fair dealing on reasonable and non-discriminatory rates, terms, and conditions with messaging ecosystem stakeholders and to operating the registry in good faith.

7 Unwanted Messaging Traffic Threat Containment

7.1 Core Principles

It is in the best interests of Consumers and all members of the wireless messaging ecosystem to enable Consumers to freely exchange wireless messages with other Consumers and Message Senders while endeavoring to eliminate threats of Unwanted Messages.

Wireless messaging is a trusted and convenient communications platform among Consumers and Message Senders. The immediacy, retrieval capabilities, storage capabilities, and high open rates associated with wireless messaging services make wireless messaging an ideal medium for all sorts of communications – including relaying urgent information to Consumers (e.g., fraud alerts or flight changes). This high trust and open rate is associated with the spam-free environment of messaging.

Unwanted Messaging traffic or reduction in reliable delivery diminishes Consumer trust in the wireless messaging ecosystem. It is vital that wireless messaging ecosystem stakeholders work together to keep the relatively pristine wireless messaging environment free of Unwanted Messages while taking steps to support the exchange of wanted wireless messages among Consumers and Message Senders.

The following core principles help ensure that Consumers are protected from Unwanted Messages:

- All Service Providers should use reasonable efforts to prevent Unwanted Messages from being sent by or to Consumers;
- All Service Providers may filter or block Unwanted Messages before they reach Consumers;
- To the extent practical and consistent with Service Providers' Unwanted Message prevention and mitigation methods, Service Providers may notify the Message Sender sending Unwanted Messages when Service Providers block Unwanted Messages;
- Service Providers should adopt Unwanted Messaging traffic practices that protect Consumers in a manner that facilitates the exchange of wanted wireless messaging traffic; and
- Where appropriate, wireless ecosystem members should collaborate to maintain Consumer trust and confidence in wireless messaging services.

7.2 Unwanted Messaging Traffic Containment and Redress Best Practices

7.2.1 Consumer Tools to Mitigate Unwanted Messaging Traffic

7.2.1.1 **Consumer Tools for Blocking or Filtering**

Consumers may choose to block Unwanted Messaging traffic. Service Providers may provide tools for Consumers to manage the messages from specific telephone

numbers they receive, filter, or block, including from those sending Unwanted Messages.

7.2.1.2 **Reporting Unwanted Messaging Traffic**

Consumers should be able to report Unwanted Messages to their Service Provider. Service Providers may establish and maintain a system to receive complaints identifying Unwanted Messages (e.g., 7726 (SPAM) reporting systems).

7.2.2 **Communication Among Service Providers**

Service Providers may communicate as appropriate to help mitigate Unwanted Messaging issues, but such communications need to be consistent with Service Providers' Unwanted Message prevention and mitigation systems, policies, and processes.

7.2.3 **Blocking Unwanted Messages and Senders**

Service Providers should adopt Unwanted Messaging traffic practices that protect Consumers in a manner that facilitates the exchange of wanted wireless messaging traffic. Service Providers may block or filter message traffic to protect Consumers, their networks, and the messaging ecosystem from Unwanted Messages. To the extent practical and consistent with Service Providers' Unwanted Message prevention and mitigation methods, Service Providers may notify the Message Sender sending Unwanted Messages when Service Providers block Unwanted Messages. Additional best practices related to the blocking of Unwanted Messages can be found in the Messaging Security Best Practices.

7.2.4 **Suspending and Disconnecting Unwanted Messaging Traffic**

Service Providers may suspend the exchange of messaging traffic with or disconnect another Service Provider when, in their discretion, such action is appropriate to stop the flow of Unwanted Messages. Notice of any such suspension might, depending on the circumstances, be provided to an impacted Service Provider through appropriate operational or business channels.

7.2.5 **Transparency of Traffic**

To protect the wireless messaging ecosystem from repeat offenders sending Unwanted Messages, Service Providers may consider assigning a unique identifier to and/or using other processes and tools for Message Senders.

7.2.6 **Mitigating Unwanted Message Issues**

Message Senders and the Service Provider to which they submit messages should take reasonable and prompt actions to resolve Unwanted Messaging issues.

7.2.7 **Network Operations Center**

Service Providers should maintain a Network Operations Center (NOC) in service.

7.2.8 **Redress**

Service Providers, Aggregators, Cloud-Based Providers, and other entities should provide a point of contact to their customers to address questions about suspected erroneous blocking from

Message Senders that can provide evidence that their messages have been blocked between message submission and receipt by the intended recipient's device.