AVAYA CPaaS™
SMS/MMS Requirements
and Code of Conduct
Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials.

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR Installs AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL Partner (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER, AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a dif-
different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE.
ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.
Table of Contents

9  CODE OF CONDUCT

10  BEST PRACTICES FOR SENDING MESSAGES
10  Consent
10  Revoking Consent (opt-out)
11  Consumer notification

12  OPT-OUT KEYWORDS AND MESSAGE
12  Opt-out confirmation message:

13  OPT-IN KEYWORDS AND MESSAGE
13  Opt-in confirmation message:

13  EXPECTATION UPON RECEIPT OF OPT-OUT/OPT-IN
13  Sending to a consumer that has opted out

14  RECOMMENDATIONS FOR CONTENT CREATION

15  DISALLOWED SENDING PRACTICES

16  DISALLOWED CONTENT

17  MONITORING
17  Consumer complaints
17  Real-time content analysis
Code of Conduct

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

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

2. The consumer must give appropriate consent for the given message type.
   Recipients of the message senders text messages must have expressed consent or "opted-in" to receiving text messages.

3. Consumer opt-in and opt-out must work correctly.
   Consumer opt-in and opt-out functionality is enforced at the network level via the STOP and UNSTOP keywords. This functionality cannot be disabled for service providers or message senders. Message senders have additional obligations for processing of opt-out messages that must be honored.

4. Phishing, spam, and unwanted illicit content is prohibited.
   Message content that deceives or threatens consumers, including phishing, is not permitted. Even if a consumer consents to receive messages, the messages must not be deceptive; TCPA compliance alone does not satisfy this condition.

5. Creative methods to evade these requirements is prohibited.
   The spirit of these requirements is straightforward; to protect both consumers and networks. Message senders acting in bad faith to thwart or undermine the spirit of these requirements are addressed on a case-by-case basis.
Best Practices for Sending Messages

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

Consent

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

<table>
<thead>
<tr>
<th>TYPES OF MESSAGING CONTENT &amp; REQUIRED CONSENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conversational</td>
</tr>
<tr>
<td>Conversational messaging is a back-and-forth conversation that takes place via text. If the consumer texts into the business first and the business responds quickly with a single message, then it's likely conversational. If the consumer initiates the conversation and the business simply responds, then no additional permission is required.</td>
</tr>
<tr>
<td>• The first message is always sent by the consumer</td>
</tr>
<tr>
<td>• Two-way conversation</td>
</tr>
<tr>
<td>• Message responds to a specific request</td>
</tr>
<tr>
<td>• The first message is sent by the consumer or business.</td>
</tr>
<tr>
<td>• One-way alert or two-way conversation</td>
</tr>
<tr>
<td>• Message contains information</td>
</tr>
<tr>
<td>• The first message is sent by the business</td>
</tr>
<tr>
<td>• One-way alert</td>
</tr>
<tr>
<td>• Message promotes a brand or product</td>
</tr>
<tr>
<td>• Prompts consumer to buy something or go somewhere</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IMPLIED CONSENT</th>
<th>EXPRESS CONSENT</th>
<th>EXPRESS WRITTEN CONSENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the consumer initiates the text message exchange and the business only responds to each consumer with relevant information, then no verbal or written permission is required.</td>
<td>The consumer should give permission before a business sends them a text message. Consumers can give permission over text, on a form or website, or verbally. Written permission also works.</td>
<td>The consumer should give written permission before a business sends them a text message. Consumers can sign a form or check a box to allow promotional text messages. Participation in text promotions should never be a requirement.</td>
</tr>
</tbody>
</table>

Revoking Consent (opt-out)

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

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

The best practice is to notify the consumer of their ability to opt-out from future messages from the message sender. This is especially important when sending informational or promotional messages. An example would be to include the sentence, “Reply STOP to unsubscribe” to the end of the initial message sent to the consumer. We recommend sending this communication on at least every 5th informational or promotional message for continued consumer awareness.
Opt-out keywords and message

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

Important: Do not include the quotation marks in the message.

Examples of valid opt-out messages:

• STOP
• Stop
• stop
• STop

Examples of invalid opt-out messages:

• Hey can you stop texting me?
• Stop it
• “Stop”

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

Opt-out confirmation message:

NETWORK MSG: You replied with the word "STOP" which blocks all texts sent from this number. Text back "UNSTOP" to receive messages again.
Opt-in keywords and message

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

Important: Do not include the quotation marks in the message.

Examples of valid opt-ins:

• UNSTOP
• Unstop
• unstop
• UNStop

Examples of invalid opt-ins:

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

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

Opt-in confirmation message:

NETWORK MSG: You have replied “unstop” and will begin receiving messages again from this number.

Expectation upon receipt of opt-out/opt-in

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

Sending to a consumer that has opted out

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

We recommend the following best practices when generating content and choosing source phone numbers. High quality, well-formatted content is more likely to be opened and read by a consumer and less likely to be mistaken for spam by Consumers, Operators, and Carriers. These best practices make messages more valuable to consumers and less likely to trigger real-time content analysis from flagging messages incorrectly as spam.

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

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

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

4. Direct consent
   You should collect the consumer consent yourself, and not use consent acquired from a third party. The consumer is expecting a relationship with the business they interacted with.

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

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

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

1. Continued sending to opted out consumers
   When a consumer opts out, they should no longer receive messages from that message sender. If they do receive messages, then it’s likely that the opt-out event was either not processed or processed incorrectly within the message sender’s network.

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

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

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

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

If a message sender is observed sending any of the below listed disallowed content, then an account review is performed. This review can result in the suspension of sending rights for a provisioned phone number; restriction of high-throughput access; suspension of provisioning rights for new phone numbers; and/or suspension of all network services. Message senders are expected to enforce restrictions on their own networks to prevent these types of content at the intake source.

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

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

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

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

Consumer complaints

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

Carriers monitor consumer complaints sent to this service for numbers on the network. If multiple complaints are received for a sender, then a notification is sent to the message sender that includes the source phone number, destination phone number, timestamp, and original message ID that was given to the message sender upon message submission.

Upon receipt, the service provider must provide proof of TCPA compliant opt-in for those specific messages. They must also provide an overview of the messaging campaign and the opt-in process that the unwanted message was a part of.

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

Real-time content analysis

Real-time analysis is used by carriers to identify if a message falls outside of the code of conduct or best practices.
## APPENDIX A: REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Release</th>
<th>Change Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>18 January, 2019</td>
<td>1.0</td>
<td>Initial document release.</td>
</tr>
<tr>
<td>25 February, 2019</td>
<td>1.1</td>
<td>Update.</td>
</tr>
<tr>
<td>12 March, 2019</td>
<td>1.2</td>
<td>Updated terms for opting out.</td>
</tr>
</tbody>
</table>