Code of Conduct

Version 2.2

November 2020

Introduction

The T-Mobile Commercial Messaging network supports more traffic throughput than a traditional person to person text messaging channels. It's designed to facilitate high-quality, high-integrity business communications, not SPAM or unconsented messaging. To protect both networks and consumers from abuse, T-Mobile enforces a basic code of conduct and provides best practices for message sending and content generation. All users of the T-Mobile network including users of the software, API, or gateway services are held to the same standards and expectations.

Contents

1 ABOUT THESE GUIDELINES

T-Mobile USA, Inc., and its affiliated brands ("**T-Mobile**"), strives to protect its Customers and provide a supportive environment for messaging services. The Code of Conduct (the "**Guidelines**") are a supplement to the most recent CTIA Short Code Monitoring Handbook as well as the CTIA Messaging Principles and Best Practices (the "**CTIA Handbook**"), as well as the Provider's Master Direct Messaging Agreement with T-Mobile (the "**Agreement**") and any additional applicable documentation and technical documentation related to T-Mobile platforms. This service is delivered via a unique 10 digit numerical code (the "**Long Code**" or the "**Toll-Free Number**") or a unique five or six digit numerical code (the "**Short Code**") owned or leased by the Provider or Content Provider to facilitate the delivery of each such messaging service (the "**Messaging Program**") through the wireless network. To the extent of these Guidelines and the CTIA Handbook conflict, these Guidelines will take precedence.

T-Mobile's requirements for supporting messaging programs on Shortcode, Longcode, and Toll-Free our on the T-Mobile network are outlined in these Guidelines.

Direct Connection Aggregators who have signed an agreement with T-Mobile, (the "**Direct Connected Aggregator or DCA**") to provide Messaging Programs on behalf of 3rd party companies or entities (the "**Content Providers**") to T-Mobile Customers, are expected to ensure that each Messaging Campaign is completely compliant with all legal requirements. Each DCA is solely responsible for the actions of their associated Content Providers and any company or entity that markets Messaging Campaigns ("**Marketing Affiliate**") on behalf of the Provider or their associated Content Providers.

These Guidelines are not intended to be a comprehensive guide for compliance with laws and regulations that apply to messaging campaigns. T-Mobile makes no representation that meeting these Guidelines or acquiring T-Mobile approval will be enough to ensure compliance with all applicable international, federal, state/local laws, ordinances, regulations, and orders ("**Applicable Laws**"). T-Mobile's "approval" of a messaging campaign is not a guarantee or an endorsement of the Messaging Program; it is reliant upon the accurate and complete disclosure of the messaging campaign as entered into by the Providers and is only intended to confirm that the description of the Messaging Campaign meets the requirements outlined in these Guidelines. T-Mobile strongly recommends that Providers and their associated Content Providers consult independent legal counsel to ensure that messaging campaigns meet the requirements of the Agreement and Applicable Laws.

The terms of this document do not limit, restrict, or waive any of T-Mobile's rights and remedies under the Agreement and that T-Mobile may change its current processes at any time with or without notice to the Provider.

1.1 COMMON TERMS

Term	Description
Aggregator or Direct Connected Aggregator (DCA)	TMUS partner who leverage the SDG system on the behalf of other message service providers and/or brands.
Application Address	The number used to support messages to and from DCAs and subscribers. Application address can come in the form of a 5-6 digit shortcode, toll-free number, or 10-digit longcode.

Term	Description
Content Provider	The actual brand/entity that is crafting the message content payload to the subscriber.
Long Code (10DLC)	A 10-digit phone number used for non-consumer messaging.
Service Provider	A general term defining an entity that provides message services for brands.
Shared Application Address	When multiple Content Providers share the same application address given each Content Providers have capabilities to custom craft a unique content message.
Shortcode	A five- or six-digit number leased from the CSCA Registry.
Toll-Free	10-digit phone numbers with the prefix of area code starting in 800, 833, 844, 855, 866, 877, 888

1.2 References

These Guidelines will continue to evolve as needed to support the best customer experience. In addition to these Guidelines, Providers and their associated Content Providers should also consult the latest versions of the following documents:

- Mobile Marketing Association's Consumer Best Practices v7.0;
- CTIA Short Code Monitoring Handbook
- CTIA Messaging Principles and Best Practices, July 2019
- California Attorney General Kamala D. Harris's "Privacy on the Go: Recommendations for the Mobile Ecosystem" best practices;
- Telephone Consumer Protection Act (TCPA) and associated case law; and
- Florida Attorney General's requirements for mobile content.

The above list is not intended to be exhaustive, and Content Providers and DCAs will need to thoroughly research other Applicable Laws or guidelines that may apply to their particular use.

1.2 Scope and Objectives

In designing these policies and best practices, T-Mobile strives to:

- Protect subscriber from unwanted messaging while providing growth for the messaging ecosystem;
- Design minimal, common-sense policies;
- Empower consumer choice;
- Support transparency and open communication with businesses; and
- Stay flexible, so that rules can adapt and evolve.

Although these best practices do not offer legal advice or guidance, the messages sent through the T-Mobile network should operate consistent with relevant laws and regulations, including (but limited to) the FCC regulations and the Telephone Consumer Protection Act (TCPA).

1.3 Enforcement

T-Mobile may, at its discretion, review content for compliance with these policies and best practices may result in the following:

- Non-compliance could result in the suspension of sending rights for a provisioned shortcode, longcode or Toll-Free numbers;
- Restriction daily quota message buckets for 10DLC services;
- Suspension of provisioning rights for new phone numbers; and/or
- Suspension of all network services.

Repeated non-compliance with these policies may result in the termination of all network services.

1.4 Revisions of Documentation

This guide is a living document and as needed will be updated and distributed accordingly by the T-Mobile business team and stakeholders. T-Mobile may update these guidelines at any time, in T-Mobile's sole and absolute discretion.

2 T-MOBILE COMPLIANCE PRINCIPLES

2.1 Sanctioned Messaging Paths and Types

T-Mobile supports commercial messaging traffic today on three dedicated paths: Shortcodes, Toll-Free, and Longcode. All commercial messaging traffic commonly referred to as non-consumer traffic must be protected from SPAM and malicious malware. All messaging partners are obligated to support basic safeguards for non-consumer traffic.

2.2 Valid Companies In Good Standing

To protect the integrity of text messaging networks and services, Content Providers who are known as the actual brand/entity crafting the message must go either a DCA validation or 3rd party validation during onboarding and maintain good standing.

2.3 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 reinforces requirements for the opt-in and opt-out mechanisms. In addition, federal laws, including the Telephone Consumer Protection Act (" TCPA"), exist to protect consumers from unwanted calls or text messages. Businesses that send text messages to consumers should have a prior relationship with the consumer and have direct opt-in to send messages to their device. T-Mobile takes violations of the TCPA a very serious matter. Should T-Mobile identify a message sender sending messages that are in direct violation of TCPA, T-Mobiles reserves the right to disable the messaging campaign immediately.

2.4 Choice and Consent

Support of advertising that is misleading or harmful to T-Mobile Customers may result in termination of the specific Messaging Program, the entire Application Address, or termination of the Agreement.

The message sender must obtain proper consumer consent for each messaging campaign sent. The type of consent required depends on the type of messaging content sent to the consumer. **Table 1-1** "Types of Messaging Content & Required Consent" describes 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 supporting universal "Stop" languages best practices unless legal authority or obligation to provide the message dictates otherwise.

The consumer must give the appropriate consent for the given message type. Where consent is required, the proposed entities authorized to send must be clearly communicated before obtaining consent, and Consumer' consent must explicitly name the entities authorized to send. Such consent may not be obtained using deceptive methods.

The content provider shall send a confirmation message upon receiving consent from the consumer. If you do not send an initial message to that individual within 30 days of receiving consent, then you will need to reconfirm consent by requesting a double opt-in. (see "Double Opt-in" below).

Once consent is received, consent applies only to the messaging program the consumer has consented too. Content providers must not treat consent as a blanket consent allowing other messaging from different brands or campaigns. A unique consent is required and is at the content provider's responsibility to obtain.

Table 1-1 – Types of Messaging Content & Required Consent

Conversational	Informational	Promotional
Conversational messaging is a back-and-forth conversation that takes place over text. If the consumer texts into the business first and the business responds quickly with a single message, it's likely conversational. If the consumer initiates the conversation and the business simply responds, no additional permission is required.	Informational messaging is when a consumer gives a business their number and asks to be contacted in the future. Appointment reminders, welcome texts, and alerts fall in this category because the first text sent by the business fulfills the consumer's request. A consumer should agree to receive texts when they give the business their mobile number.	Promotional messaging is when a message contains a sales or marketing promotion. Adding a call-to-action like a coupon code to an informational text may place it in the promotional category. Before a business sends promotional messages, the consumer must agree in writing to receive promotional texts. Businesses that already ask consumers to sign forms or submit contact information can add a field to capture consent.
The first message always sent by the consumer Two-way conversation Message responds to a specific request	The first message is sent by the consumer or business One-way alert or two-way conversation Message contains information	The first message is sent by the business One-way alert Message promotes a brand or product Prompts consumer to buy something or go somewhere
IMPLIED CONSENT If the consumer initiates the text message exchange and the business only responds to each consumer with relevant information, no verbal or written permission is required.	EXPRESSED CONSENT The consumer should grant permission before the business texts them. They can grant permission over text, on a form or website, or verbally. Written permission also works.	EXPRESSED WRITTEN CONSENT The consumer should give written permission before a business text them. They can sign a form or check a box to allow promotional text messages. Participation in-text promotions should never be a requirement.

2.5 Calls-to-Action

Content Providers 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's consent to receive a message is explicitly clear and informs them of the nature of the program.

Content providers 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 Application Address from which the 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).

2.6 Opt-In

Content Providers 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).

Below are only examples of how a consumer may demonstrate their opt-in consent to receive messaging traffic for the designated campaign. The examples include but are 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.

At any time, T-Mobile may request proof of consumer opt-in. It is the DCA and their content provider requirement to pride opt-in consent records along with the method of how opt-in was obtained (i.e. Shortcode keyword, website URL, etc.). Below are examples of documented opt-in consent data acceptable by T-Mobile.

- The timestamp of consent acquisition;
- Consent acquisition medium (e.g., cell-submit form, physical sign-up form, SMS keyword, etc.);
- The 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;
- The 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 username, session ID, etc.)).

2.7 Double Opt-In

T-Mobile does recommend obtaining a secondary "Double Opt-In" in cases where the consent was initially collected outside of SMS channels, (i.e. phone call, web form, POS, etc.). Double Opt-In is the practice of confirming an opt-in via text by requesting the consumer to reply "Yes" to confirm in participating in a text messaging with the business. This gives the business confidence in receiving proper subscriber consent and protecting against incorrect mobile number collection. Additionally, there are use cases outlined in this code of conduct that require a double opt-in to proceed with sending messaging to consumers.

Examples of Double Opt-In:

- "Reply Yes to confirm that you want to receive text messages from {Business Name}, Reply STOP to unsubscribe"
- "{Brand Name}: Reply YES to confirm receiving SMS/MMS messages {Link to Terms of Service} Reply "STOP" to unsubscribe"

2.8 Opt-Out

Functioning opt-out mechanisms are crucial for all text messaging programs. Programs must always acknowledge and respect customers' requests to opt-out of programs. Messaging programs must respond to, at a minimum, the universal keywords STOP, END, CANCEL, UNSUBSCRIBE, and QUIT by sending an opt-out message and, if the user is subscribed, by opting the user out of the program. Subsequent text, punctuation, capitalization, or some combination thereof must not interfere with opt-out keyword functionality. Recurring-messages programs must also display opt-out instructions at program opt-in and regular intervals of content service messages, at least once per month. Opt-out information must be displayed in the advertisement or within the terms and conditions.

A program should deliver one final message to confirm a user has opted out successfully, but no additional messages may be sent after the user indicates a desire to cancel a message program.

Additionally, Content providers should acknowledge and respect Consumers' opt-out requests consistent with the following guidelines:

- Message Senders should ensure that Consumers can opt-out of receiving messages at any time;
- Message Senders should support multiple mechanisms of opt-out, including phone call, email, or text;
- A messaging campaign should deliver one final message to confirm a user has opted out successfully, but no additional messages may be sent after the user indicates a desire to cancel from receiving further messages.

A "high" volume or percentage of opt-out messages may result in suspension or termination of a specific messaging campaign and/or blocking of sending numbers.

2.9 Aggregator Enforced "STOP" Layer

T-Mobile suggests DCA support mandatory opt-out compliance by supporting the STOP keyword at the network level. This opt-out system should be active by default and across all Content Providers/Messaging Senders on the Aggregator bind. Otherwise referred to as a "STOP Layer", a STOP request blocks all text message exchanges between a consumer and a content provider's messaging campaign. A consumer can opt back in at any time by re-opting into the messaging programs via the call-to-action.

2.10 Consumer Notification

T-Mobile recommends the best practice of notifying the consumer of its ability to opt-out from future messages from the Content Provider. 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 message sent to the consumer. We recommend sending this communication on the first message and at least every 5th message or at least once a month for continued consumer awareness, if not on every message.

2.11 Opt-Out Keywords and Message

A consumer can opt-out of communication with any content provider by texting any universal STOP Keywords (Stop, End, Quit, Unsubscribe, Cancel). The most common keyword is “STOP”. 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 should also be honored. There may be some use cases when a MO response triggers an opt-out keyword where the intention is not to opt-out but rather respond or request for help. In this instance, it is up to the content provider to determine if the consumer is intending to request opt-out or likewise.

Examples of valid opt-out keywords:

- “STOP”
- “Stop”
- “stop”
- “STop”

Examples of valid opt-out messages:

- "please stop texting me"
- "you have the wrong number, stop"
- “Stop it!”

Examples of invalid opt-out messages:

- “Hey, my subscription ended, how do I renew?”
- “I cannot get my device to stop, can you help?"

2.12 Sending To A Consumer That Has Opted Out

If a message sender attempts to send an SMS message to a consumer that has opted out of communications with the messaging campaign T-Mobiles reserves the right to disable the messaging campaign at the risk of the message sender and conduct a full consent audit.

2.13 Deactivation Files

To ensure that messages are not sent to phone numbers that were canceled by the wireless consumer user who initially opted in and subsequently reassigned to a new wireless consumer, message senders must process the T-Mobile Deactivation Files (MDNs) daily. DCA and Content Providers assume responsibility for managing information about deactivated and recycled mobile phone numbers. Aggregators must either enforce deactivations files themselves or ensure that deactivation information is made available to Message Senders. Failure to process deactivated MDNs may lead to excessive consumer complaints and SPAM. T-Mobiles reserves the right to disable the messaging campaign at the risk of the message sender and conduct a full consent audit if a Content Provider is found not processing deactivation files.

2.14 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 (e.g. in the case of an opt-out request) and Consumer consent is honored to minimize Unwanted Messages. Message Senders should process Mobile Deactivation Files daily and remove any deactivated telephone numbers from any opt-in lists.

2.15 High Opt-Out Rates

Messaging campaigns that yield high opt-out rates may suggest compliance issues with the campaign, content provider, or opt-in list. DCA should monitor STOP and HELP responses on a campaign basis and should be flagged for monitoring and/or conduct a consent audit shall opt-out rates exceed .5% per messaging campaign blast. The daily opt-out rate on a messaging campaign is defined as the total number of unique consumer phone numbers divided by the unique opted out consumers that were sent messages within 24 hours.

Additionally, it is suggested if opt-out rates exceed greater than 4% opt-out within 24 hours immediate suspension of the messaging campaign, root cause analysis (RCA) of issue and consent audit should be triggered. At T-Mobile's discretion, any campaign found to have a "high" volume or percentage of opt-out messages and or complaints may result in suspension or termination of a specific messaging campaign and/or blocking of sending numbers.

3 BEST PRACTICES FOR MESSAGING PROGRAMS

T-Mobile recommends the following best practices when sending non-consumer messages to the T-Mobile Network. High quality, well-formatted content is more likely to be opened and read by a consumer and less likely to be mistaken as SPAM by consumers, T-Mobile, and messaging ecosystem.

The best practices below are intended to make messages more valuable to consumers and less likely associated incorrectly as SPAM.

3.1 Use One Recognizable Source Number (Application Address)

Each business or program should use one primary number (Shortcode, Longcode, or Toll-Free number). Using a single number for both text and voice calls is recommended. A business should run all their business traffic on one phone number and avoid using multiple numbers for the same messaging campaign. The use of multiple numbers is not prohibited however please note will not provide additional volumes of traffic or throughput on the T-Mobile network.

3.2 Enabling Voice Components

Businesses who are only interested in messaging campaigns are suggested to enable voice recording on the Longcode or Toll-Free number for better consumer experience. Shall a consumer call the phone number of the content provider and receive an error "this number is not in service" message they will be more likely to flag and report as SPAM. If the content provider does not wish to enable voice service, it is suggested to consider a voicemail message including the business name and directing the consumer back to the messaging experience.

3.3 Use One Recognizable Domain Name

Each program should be associated with a single business's web domain. Although a full domain is preferred, a branded short URL may be used to deliver custom links. This adds continuity with the consumer to improve brand awareness as well as increases confidence in the link.

3.4 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 and should be avoided.

3.5 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. Please refer to section 2.4 for further information on consent.

3.6 Set Expectations On Frequency

Content Providers should set the proper expectation with the consumer on how many messages they can expect to receive. If you are sending 5 texts a month, then disclosing "5/msg a month" on the first interaction will result in a positive consumer experience.

3.7 Business Recognition

You should include the business name within the message to ensure that the consumer knows who they are interreacting and not attempt to hide the identity.

3.8 Length of Message

SMS stands for "Short Message Service" and this should be taken into consideration when formatting a text message. Even though concatenated messages are supported on the T-Mobile network we recommend keeping messages smaller than 160-characters in length for better customer experience.

3.9 Ending with "Stop" and "Help"

To ensure that the consumer feels that they have control to remove themselves from text message communication, you should send your messages with the Opt-out keyword "Stop". To ensure that the consumer feels that they can receive assistance in the messaging program you should end messages with the keyword "Help" to receive help.

3.10 Transitioning Messaging Programs to a New Application Address:

To protect and preserve Consumers' trust in Messaging programs, Message Senders must disclose when a recurring-messages program will transition from one application address (10DLC, Shortcode, or Toll-Free) to another. Additionally, a new opt-in must occur on the new application address to ensure consumer consent has been acquired. Below is the following process

To transition a recurring-messages program the following steps should be followed:

1. On the old application address, send a final Service Message to Consumers enrolled in the recurring-messages program. The final Service Message must disclose:
    - The number for the new application address that will be used for the recurring-messages program;
    - The recurring-messages program's name or product description;
    - Opt-out information; and
    - Other important details regarding the transition (e.g., customer care contact information).

2. Content Providers must send a second message within 24 hours on the new application address. This message must include:
    - The recurring-messages program's name or product description;
    - Opt-out information;
    - Customer care contact information; and
    - Message frequency disclosure.

    If a consumer responds with a universal stop command or like words, the Content Provider must cease to send messages.

3. Immediately discontinue the recurring-messages program on the old application address.

3.11 Expiring a Messaging Program

The provider must expire all messaging campaign that is no longer functioning in the market. It is the responsibility of the Aggregator and Service provider to ensure T-Mobile's messaging to up to date in the applicable registries and T-Mobile system.

3.12 Campaigns Information Accuracy

Providers must keep all messaging campaigns accurate to what is live in the market. Shall a messaging campaign be supporting messaging traffic not registered within T-Mobile, T-Mobile reserves the right to immediately suspend a messaging campaign at the expense of the Content Provider.

4 PROHIBITED MESSAGING PRACTICES

Service Providers should refrain from disingenuous sending practices. Service Providers are expected to enforce restrictions on their networks to prevent the disallowed sending practices listed below:

4.1 Sharing, Selling or Renting Consent is prohibited

T-Mobile in no way allows consumers' consent to be bought, sold, rented, or shared.

4.2 Grey Route

Aggregators and Company's Content providers are prohibited from utilizing Grey Routes to send Non-Consumer (A2P) messages. A Grey Route is a setting, method, or path that is not authorized by Service Providers for Non-Consumer Messages.

4.3 Snowshoe Sending Prohibited

Snowshoe sending is defined as a technique used to spread messages across many source phone numbers, specifically to dilute reputation metrics and evade filters. T-Mobile actively monitors for snowshoe sending. If discovered, T-Mobile reserves the right to disable the messaging campaign at the risk of the message sender and further messaging campaigns may result in immediate suspension.

Messaging use cases that require the use of multiple numbers to distribute "similar" or "like" content may request special approval through an approval T-Mobile process.

4.4 Filter Evasion Assistance Prohibited

Sending mechanisms designed to evade SPAM controls are prohibited. Aggregators and Service providers are expected to work with T-Mobile to resolve SPAM and unwarranted blocking issues. The practice of automatically providing a sender with new phone numbers to replace phone numbers blocked by a receiving network is specifically prohibited.

4.5 Dynamic Routing Prohibited

Each 10DLC, Shortcode, and Toll-Free number must have a single route in the delivery path to the destination phone number. Routing is expected to change infrequently, typically as a result of changing contractual relationships, rather than dynamically. If the Aggregator and or Messaging sender is identified as preforming dynamic routing as means to circumvent SPAM blocking T-Mobile reserves the right to disable the messaging campaign at the risk of the message sender and further messaging campaigns may result in immediate suspension. Dynamic Routing to maintain service in the event or major network outage on the Service provider's side is not prohibited.

4.6 Shared Codes Prohibited

Shared 10DLC, shortcodes, and Toll-Free numbers are prohibited. A Shared Code is defined when multiple Content Providers share the same application address given each Content Providers have capabilities to custom craft a unique content message.

10DLCs & Toll-Free

The use of shared telephone numbers across multiple businesses, entities, or organizations is prohibited. "Sub-aggregating" a single telephone number with multiple Message Senders is also prohibited. Content Providers may require special business review and approval from T-Mobile for consideration of share-telephone numbers that may be specific to Enterprise based use-cases. In instances where a shared number use is approved, all Message Senders operating on a shared number should be documented and available, by the designated T-Mobile onboarding process.

Shortcodes

Effective immediately no new shared shortcodes are allowed to be onboarded. All existing shared shortcodes will be required to migrate at a future date to a dedicated application address (Shortcode, 10DLC, or Toll-Free). Formal communication with appropriate advance notice will be provided.

4.7 URL Cycling / Public URL Shorteners

The practice of using multiple FQDNs (i.e. host.domain) in bulk messaging with similar message content (e.g., for the specific purpose of evading filters and/or diluting reputation metrics) by a single party is prohibited.

The practice of using public URL shorteners in bulk messaging is highly discouraged, and messages containing them may be subject to blocking. The practice of using multiple public URL shorteners (i.e. host.domain/path) in bulk messaging with similar message content (e.g., for the specific purpose of evading filters and/or diluting reputation metrics) is prohibited.

Messaging use cases that require the use of multiple numbers to distribute "similar" or "like" content may request special approval through an approval T-Mobile process.

4.8 URL Redirects/Forwarding

When message senders include a URL in the message and the URL will redirect to another URL and then redirect again and so on. This practice can go multiple layers deep resulting in the consumer not knowing what website they will eventually be taken to. This sending practice may result in immediate suspension of services.

4.9 Number Cycling

Number cycling is when a message sender uses a number (normally Longcode or Toll-Free) until it begins to show signs of deliverability degradation. After which the content provider will discard the number for a new one and repeats the process. This sending practice results in poor consumer experience, suggests unwanted messaging traffic, and lack of consumer consent. If identified T-Mobiles reserves the right to disable the Content Provider/Brand at their own risk.

5 PROHIBITED CAMPAIGN CONTENT

5.1 Unlawful, Unapproved, or Illicit Content

No messaging programs can run on the T-Mobile that may promote unlawful, unapproved, or illicit content, including but not limited to:

- SPAM;
- Fraudulent or misleading messages;
- Depictions or endorsements of violence;
- Inappropriate content;
- Profanity or hate speech;
- Endorsement of illegal drugs

Programs must operate according to all applicable federal and state laws and regulations. In addition, the content must be legal across all 50 states. All content must be appropriate for the intended audience. Additional legal and ethical obligations apply when marketing to children under age 13, and such programs might be subject to additional review by T-Mobile.

Aggregators and Message Senders are expected to enforce restrictions on their networks to prevent onboarding these types of content. If determined to support any of the following restricted content T-Mobile reserves the rights to all, and not limited to, the following actions:

- Suspension of sending rights for provisioned application address or campaign;
- Restriction of onboarding new message campaigns;
- Suspension of provisioning rights for new application address; and/or
- Suspension of all network services on the T-Mobile network

5.2 Disallowed Content

The following content categories are considered deceitful and nuisance campaigns which may result in high volumes of SPAM complaints on the T-Mobile network. Due to these issues, we will no longer support any campaign under the following categories, regardless of any prior approval. Messaging use cases that support the disallowed content outlined below may request an official exception in writing by T-Mobile through an official T-Mobile exception approval process. Any exception that existed before September 1, 2020, should be considered invalid.

High-Risk Financial Services	• Payday Loans • Non-Direct Lenders • Debt Collection
Debt Forgiveness	• Debt Consolidation • Debt Reduction • Credit Repair Programs
Illegal Substances	• Cannabis • Illegal Prescriptions

Work & Investment Opportunities	• Work from Home Programs • Job Alerts from 3rd Party Recruiting Firms • Risk Investment Opportunities
Other	• Gambling • Any other illegal content • Lead generation indicate the sharing of collected information with third parties • Campaign types are not in compliance with the recommendations of or prohibited by the CTIA Short Code Monitoring Handbook, Version 1.7, or later. • Campaign types not in compliance with the recommendations of or prohibited by the CTIA Messaging Principles and Best Practices – 2019 version

5.3 Phishing

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

5.4 Fraud or Scam

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

5.5 Deceptive Marketing

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

5.6 Compliance Audits and Notices

Consumers may choose to block unwanted messaging traffic on the T-Mobile network. To protect our consumers and keep non-consumer messaging healthy T-Mobile has launched an internal compliance and policy monitoring program. In conjunction with CTIA efforts T-Mobile's program will monitor messaging campaigns and audit notices may result in violations against Industry best practices and the T-Mobile Code of Conduct.
Immediate action must take place shall external-monitoring efforts or T-Mobile-monitoring efforts to identify traffic as a potential for consumer harm. Severity-0 representing the most extreme violations. T-Mobile reserves the right to protect our consumers by turning down a messaging campaign on a case by case bases.

For Severity-0s:

- Immediate suspension of messaging campaign
- Notification to DCA of severity incident
- T-Mobile will issue an RCA document and it must be complete in its entirety
- The Messaging provider will have 24-48 hours to complete the correct action and return the RCA
- The identified root cause must be corrected to request reinstatement of the messaging program

If there are several offenses on Content Provider and/or application address, this may result in the indefinite suspension of the messaging sender and campaign(s).

5.7 Age Gating

T-Mobile may, at its discretion and at any time, suspend, terminate, or not Approve any Messaging Program it feels does not promote a legal, age-appropriate, or positive customer experience. All content must adhere to all applicable laws and support a functioning age gate when associated with but not limited to Sex, Alcohol, Firearms, Tobacco, and/or any other age-restricted content that must comply with legal regulations. Non-acceptable age gating function includes but is not limited to Yes or No responses. The age-gate mechanism should include the date of birth verification during the consent opt-in of the consumer.

6 SPECIAL USE CASES

6.1 Political Messaging

T-Mobile supports all political parties and messages to their constituents. To run political messaging, the requirements are the campaigns run on the correct non-consumer channel. We require all parties who support political messaging services to follow CTIA Messaging Principles and Best Practices, CTIA Political Campaign Messaging Document, as well as, T-Mobile Code of Conduct. We especially require any political campaigns to honor "STOP" opt-out requests from subscribers.

To run 10DLC political messaging campaigns on the T-Mobile network, a special registration and third-party verification check is required (i.e. Campaign Verify). This process is required to the ensure authenticity of the political candidate or entity.

Currently, federal-level candidates or entities (e.g. Presidential or Legislative Candidates, PACs, and Committees) are available to the registry on Campaign Verify.

Political Candidates are required to send extended information that includes the following requirements:

- Message campaign must be on a dedicated application address
- 10DLC ONLY: Confirmation of Vetting through Campaign Verify (www.campaignverify.org)
    - Campaign Verify Token
- Politician/Organization Name
- FEC Committee ID
- Politician/Organization Website

6.2 Shopping Cart Reminders

T-Mobile policy regarding shopping cart reminder notifications is as follows:

General Requirements

1. Call to Action via the website must include within the opt-in terms and conditions details that the message program includes shopping cart reminder
2. Shopping cart message program must incorporate a double opt-in mechanism via text
3. Double Opt-in message content must clearly inform the user that the message program includes shopping cart reminders
4. Campaign submissions must be filed as an "Account Information" campaign with a detailed description highlighting the message program will include shopping cart reminders

Additional Privacy Policy Disclosures

1. The privacy policy must explicitly state how information is captured by the e-commerce site to determine when a consumer cart has been abandoned (e.g. website cookies, plugins, etc.).
2. Terms and conditions must reflect the new policy

Delivery and Content Restrictions

1. Text reminders must be sent within 48 hours and limited to one alert per unique abandoned cart
2. Abandoned cart notification must not result in the e-commerce site completing the transaction on behalf of the consumer
    a. Abandoned cart notification must not collect payment information or accept approval for purchase via keyword confirmation from the consumer
    b. Consumers must complete the transaction by processing payment themselves via a direct URL link to the e-commerce website.

6.3 Free-To-End User Programs

FTEU is currently available only for Shortcode messaging programs. FTEU programs must display a clear call-to-action, capture consumers' affirmative opt-in, send an opt-in confirmation message, and abide by customers' requests to opt-out. However, all FTEU programs are exempt from displaying "message and data rates may apply" in advertisements, terms and conditions, and messages. If the content provider's messaging program needs free delivery the program must be supported on a dedicated Shortcode.

6.4 Sweepstakes and Contest

Sweepstakes are characterized by the element of chance and the awarding of a prize. Sweepstakes are governed by extensive and specific Applicable Laws. Organizations considering a sweepstakes program are urged to consult with legal counsel experienced in sweepstakes management before submitting a program for T-Mobile approval. T-Mobile requires special business review and we reserve the right to approve or reject the sweepstakes at our discretion. Note that sweepstakes program review might take longer than reviews of other program types.

6.5 IoT or M2M (Machine to Machine) Messages

IoT or Machine-to-machine (M2M) messaging programs should never interact with Consumers directly. If the Content Provider of the IoT service has a use case to support subscriber facing messaging, messages must be supported on a different dedicated code.

6.6 Controlled Substances and Adult Content

All content should be appropriate for the intended audience. Messaging content for controlled substances or distribution of adult content might be subject to additional T-Mobile review. T-Mobile retains the sole discretion to determine if the content is allowed or not. Messages should include robust age verification at opt-in (e.g., electronic confirmation of age and identity). The following is a non-exhaustive list of examples types of content not allowed under this provision:

- Content promoting underage, non-consensual, or other illegal sexual themes, whether simulated or real.
    - Examples: Rape, incest, bestiality, necrophilia, Lolita or teen-themed pornography, underage dating
- Content that may be interpreted as promoting a sexual act in exchange for compensation.
    - Examples: Prostitution, companionship and escort services, intimate massage and similar services, cuddling sites
- Content promoting the sexual exploitation of minors
    - Examples: Child sexual abuse imagery or other content
- Content that is made to appear appropriate for a family audience but contains adult themes, including sex, violence, vulgarity, or other depictions of children or popular children's characters, that are unsuitable for a general audience
- Alcohol and drinks that resemble alcohol or brands which target minors

6.7 Charitable Donation programs

T-Mobile cares about charitable donations and protecting consumers from fraudulent harm. There are two paths in which charitable donations are supported on the T-Mobile network:

1. Direct-carrier billing running on Premium Shortcode supported by T-Mobile Mobile Giving Aggregator
2. Dedicated application address with donation URL link supported by DCA

Charitable donation programs must conform to the non-profit messaging guidelines in the CTIA Messaging Principles and Best Practices. All Charitable Organizations must meet the following qualifications:

- Qualified as tax-exempt under Section 501(c)(3) of the Internal Revenue Code are eligible;
- Charitable organizations must be accredited by at least one arm's-length, disinterested non-profit accreditation organization (e.g., Better Business Bureau Wise Giving Alliance, Charity Navigator);
- Charitable organizations must receive separate opt-in for informational and solicitation messages if they provide both types of messages under the same Short Code;
- Charitable organizations may not use the message program for lotteries, sweepstakes, raffles, or recurring donations;
- No entities involved in the donation campaign, aside from the charitable organization itself, may use any part of the mobile subscriber data collected; and
- For charitable donations programs outside of direct-carrier billing, the dedicated application address must be leased/owned by the charitable organization

Furthermore, charitable donation programs supported by a DCA must provide the following requirements:

- Charitable donation campaign must be set up on a dedicated application address
- Provide the following Charitable Organization information for proof of qualified as tax-exempt under Section 501(c)(3) of the Internal Revenue Code:
    1. Name of Company/Non-Profit Organization
    2. Tax Identification (EIN)
    3. Charitable Organization Website
    4. Accreditation Organization Website Listing Company/Non-Profit

6.8 Emergency Notifications

Messaging campaign supporting emergency notifications are suggested to run on FTEU provisioned Shortcodes. If an emergency notification needs to be sent at the Federal, state, local, tribal and territorial alerting authorities it is suggested to use IPAWS/WEA and integrate local systems that use Common Alerting Protocol (CAP) standards with the IPAWS infrastructure.

- WEA is a public safety notification system administered thru FEMA's Integrated Public Alert Warning System (IPAWS) that enables authorized agencies to send text-like messages to consumers with capable wireless.
- IPAWS provides public safety officials with an effective way to alert and warn the public about serious emergencies using:
- Wireless Emergency Alerts (WEA),
- Emergency Alert System (EAS),
- National Oceanic and Atmospheric Administration (NOAA) Weather Radio, and
- Other public alerting systems from a single interface.
- T-Mobile (along with the other nationwide carriers) participate in the WEA program.